



التهديد السيبراني الإيراني

الملف المضاف الى برنامجها النووي ودوره المحتمل في تأجيج صراع من نمط جديد

حسن مظفر الرزو



الطبعة الأولى: 2020

رقم التسجيل: VR. 3373-63560 . B

المركز الديمقراطي العربي

حسن مظفر الرزو





The Iranian cyber threat

is the file added to its nuclear program and its potential role in fueling a new type of conflict

Germany: Berlin 10315
Gensinger- Str: 112
http: // democraticac.doc





المركز الديمقراطي العربي



Democratic Arab Center

Strategic, Political & Economic studies

التهديد السيبراني الإيراني

الملف المضاف الى برنامجها النووي ودوره المحتمل في تأجيج صراع من نمط جديد

The Iranian cyber threat is the file added to its nuclear program and its potential role in fueling a new type of conflict

المؤلف: حسن مظفر الرزو

إخراج و تنسيق: بن قيطة بلال

الطبعة الأولى : 2020



رئيس المركز : أ. عمار شرعان

المؤلف: حسن مظفر الرزو

عنوان الكتاب: التهديد السيبراني الإيراني – الملف المضاف الى برنامجها النووي ودوره المحتمل في تأجيج صراع من نمط جديد

إخراج و تنسيق : بن قيطة بلال

رقــم تسجيل الكتاب: VR. 3373-63560. B

الطبعة : الأولى 2020

الناشر: المركز الديمقراطي العربي للدراسات الاستراتيجية و السياسية و الاقتصادية،برلين _ ألمانيا

المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية

Germany:
Berlin 10315 Gensinger.Str: 112
Tel: 0049-Code Germany
54884375 -030
91499898 -030
86450098 -030
mobiltelefon : 00491742783717
E-mail: book@democraticac.de

الإهداء

الى

وصلة ارتباطي بالدنيا ....وغاية سلوتي فيها

ولدي محمد وابنتي مروة وآمنة

أهدي لكم ثمرة جهد أرجو أن تجديكم نفعاً

فهرست المحتويات

[1] . حرصت على إيراد الاصطلاح كما ورد باللغة الإنجليزية من الفقرة الأولى، وعدم ايراد الاصطلاح باللغة العربية لحين انجلاء الغموض عن دلالته، وانتخاب مصطلح مناسب له من لغتنا العربية، بحيث يتوافق مع مضامينه المعرفية والتقنية.

[2] . كلمة *Ashiyane* تستخدم في اللغة الفارسية وتطلق على العش أو الوكر الذي تلجأ اليه وتقيم فيه الطيور وصغارها، من أجل ذلك نلاحظ كثرة استخدام اصطلاحات صغار الطيور وأفراخها في كثير من خطابات التواصل بين أعضاء هذه المجموعة.

كشاف بأسماء مؤسسات الفضاء السيبراني الإيراني وكياناته السيبرانية

الاصطلاح	الوصف
ACRI	معهد البحوث المتقدمة في الاتصالات.
AFTA	المجلس العالي لأمن تبادل المعلومات.
AICTC	مركز البحوث المتقدمة في مجال تقنية المعلومات والاتصالات
BCC	مجلس الفضاء السيبراني في منظمة الباسيج
CCL	قانون جرائم الفضاء السيبراني.
CDICC	هيئة تقدير حالات المحتوى الجنائي.
CDS	قيادة عمليات الدفاع في الفضاء السيبراني.
CHIA	مركز فضاء معلومات الجيش الإيراني.
CISD	مركز المعلومات والوثائق العلمية.
CIUW	هيئة تمييز مواقع الويب ـ غير المرخصة.
CRA	السلطة التنظيمية لاتصالات إيران.
CRCIS	مركز بحوث الحاسب للعلوم الإسلامية.
CSIRT	فرق الاستجابة الأمنية لحوادث الحاسب.
DCC	شركة بيانات الاتصالات.
DCI	شركة إيران لتناقل البيانات.
DSRL	مخابر بحوث أمن المعلومات.
ERC	مركز بحوث الالكترونيات.
FATA	شرطة فضاء إيران السيبراني.
HALAL INTERNET	شبكة الإنترنيت الشرعية.
HCC	المجلس الأعلى لالفضاء السيبراني.
HCDP	المجلس الأعلى لمعالجة البيانات.
HCI	المجلس الأعلى للمعلوماتية.
HCID	المجلس الأعلى لنشر المعلومات.
HCIS	سكرتارية الهيئة السيبرانية العليا.
HCIT	المجلس الأعلى لتقنية المعلومات.
HCNS	المجلس الأعلى للأمن الوطني.
ICA	جيش فضاء إيران السيبراني.
ICNC	الجمعية الإيرانية للمحتوى الوطني.
ICP	وكلاء إيران السيبرانيين.

الاصطلاح	الوصف
IDRO	مركز تطوير تقنية المعلومات.
IHCI	المجلس الإيراني الأعلى للمعلوماتية.
INSF	المجلس الوطني للعلوم.
IranDoc	مركز إيران للمعلومات العلمية والتوثيق.
IRANET	شبكة معلومات واتصالات إيران.
Iranology	معهد علوم إيران.
ISP	شركات مجهزات الخدمات السيبرانية.
ISV	وادي السليكون الإيراني.
ITCE	مجلس التميز لتقنية المعلومات.
ITDI	مؤسسة تنمية تقنية المعلومات في إيران.
ITO	مؤسسة تقنية المعلومات.
ITRC	مركز إيران لبحوث الاتصالات.
KMCCF	فصائل ميليشيات كربلاء للقوى الثقافية في الفضاء السيبراني.
KVU	جامعة الخميني الافتراضية.
MAHER	مركز مهر لفرق الاستجابة الأمنية لحوادث الحاسبات.
MCIT	وزارة تقنية المعلومات والاتصالات.
MICT	وزارة المعلومات وتقنيات الاتصالات.
MISI	جمعية قياس مجتمع المعلومات في إيران.
MPTT	وزارة البريد والتلغراف والهاتف الإيرانية.
MSRT	وزارة العلوم والبحوث والتقنية.
NCC	المركز الوطني لالفضاء السيبراني.
NICTA	الوكالة الوطنية لتقنية المعلومات والاتصالات.
NIN	الشبكة الوطنية للمعلومات.
NSN	الشبكة الوطنية العلمية.
NSRC	المجلس الوطني للبحث العلمي.
OPRB	مكتب تشجيع المدوّنات الدينية.
PARSTEL	شركة إيران المتحدة للصناعات الاتصالية.
PCC	مجلس الباسيج لالفضاء السيبراني.
PDO	منظمة الدفاع المدني.
RCEICT	المركز الإقليمي للتميز في قطاع المعلومات والاتصالات.
SAPRC	مركز شريف لبحوث الفيزياء التطبيقية.
SCCPR	الهيئة العليا لتنظيم سياسة الفضاء السيبراني.

الاصطلاح	الوصف
SCCS	الهيئة العليا لأمن الفضاء السيبراني.
SCICT	المجلس الأعلى لتقنية المعلومات والاتصالات.
SCIPCC	الهيئة العليا لتحسين وإنتاج محتوى الفضاء السيبراني.
SEA	جيش فضاء إيران السيبراني.
SHETAB	شبكة النظام الجامع للمصارف الوطنية.
SHOMA	شبكة الإنترنيت الوطنية.
SOC	مركز العمليات الأمنية للبيئة الصناعية.
TAKFA	البرنامج الوطني الإيراني لتقنية المعلومات.
TBS	التواصل المصرفي عن بعد.
TCI	شركة الاتصالات الإيرانية.
TSITP	حديقة طهران للبرمجيات والمعلومات والتقنية.

توطئة

بسم الله الرحمن الرحيم

توطئة:

ارتبطت إيران بفضاء الفيض السيبراني، في البداية، من خلال ترويج خدمة البريد الإلكتروني، وخدمات رقمية أخرى، في عقد التسعينات من القرن العشرين، ومن خلال بوابات مراكز البحوث الأكاديمية والعلمية، قبل أن تنطلق خدمة الإنترنيت داخل حدود هذه المؤسسات قبل أن تنفتح على المواطنين الإيرانيين.

ورغم أن النظام قد تعامل بعفوية مع حضور فضاء الإنترنيت في البلاد، إلا أن أصوات المعارضين الذين يمثلون المؤسسات الأمنية، والكيانات الحوزوية، قد تعالت معترضة على المحتوى المطروح في بعض المواقع، والذي يعارض خطاطة ثقافة الثورة الإسلامية أو يهدد أمنها.

ورغم مرور أكثر من عقد على دخول إيران في الفضاء السيبراني العولمي، وانتشار الكثير من تطبيقاته، وخدماته، وولادة كيانات رقمية محلية التحقت بنسيج الفضاء العولمي فلم ينجح النظام الإيراني في تحقيق توازن موضوعي بين مسألة الأمن السيبراني الوطني وبين توفير فرصة سانحة لمواطنيه في ممارسة حقهم المشروع بالإبحار بين مواقع الويب المقيمة في فضاء الفيض السيبراني لشبكة الإنترنيت. وبقي النظام يكابر فلا يقبل الاعتراف أن ثمة قيود جائرة باتت الحكومة الإيرانية ومؤسساتها الأمنية تفرضها على المستخدمين، وتحظر عنهم الكثير من المواقع، مع الاستمرار بإحباط الخطاب التواصلي مع الآخر، الذي لم يستطيع النظام أن يتصالح مع أي مستوى من مستويات خطابه المعرفي، والسياسي، والعقدي . وبدا جلياً أن مثل هذه المكابرة، غير المبرّرة قد كلفت النظام حجماً كبيراً من التخصيصات الاستثمارية لتمويل مشاريع غير مسبوقة في مجتمع المعلومات المعاصر، فعمدت الى اصطناع فضاء رقمي منغلق على غير الإيرانيين عبر مشروع الإنترنيت الحلال *SHOMA* الذي لا زال يتعثر بين الحين والآخر، مع استمرار تأخير نقطة انطلاق المشروع بصورة متكاملة.

كذلك فإن توظيف أكثر أنظمة الكف والحظر السيبراني صرامة، مع تتبع جميع نبضات الفيض السيبراني المسافر من والى فضاء إيران قد نشب عنه حصول تباطؤ ملحوظ في الخدمة، مع استبعاد الكثير من مادة المحتوى السيبراني المطروح في فضاء الإنترنيت نتيجة للفجوات التي تعاني منها نظم الترشيح الكي لعبارات تستغلق على منطقها البرمجي فتعمد الى إدراجها بقائمة المحظور.

فتحول فضاء الفيض السيبراني من فضاء متنوع، يحفل بجميع مفردات الحضور الإنساني في إيجابياته وتناقضاته الى فضاء سياسي يقلق النظام الإيراني، ويستأثر حجماً كبيراً من اهتمامات مؤسساتها الأمنية والعسكرية لكونه يمثل، وفق رؤيتهم، قناة مفتوحة للتسلل الى عمارة ثقافة الثورة الإسلامية، ومصدراً لتهديد مكاسبها.

ومما زاد الطين بلّة هو حرص الولايات المتحدة وإسرائيل على تصعيد هذه الفوبيا بعد أن استثمرت هذا الفضاء في شنّ هجمات اكتسحت من خلالها جميع الحصون السيبرانية لمشروع إيران النووي، فبلغت أجهزة الطرد المركزي وتسببت في إيقاف الكثير منها عن العمل. فتصاعد القلق الإيراني الى أعلى مستوياته وتعمّقت القناعة بالبعد السياسي

والعسكري، والأمني الذي يمكن أن يمارسه هذا الفضاء، فوسعت دائرة اهتمامها بجلّ تفاصيل، وسخّرت له موارداً مالية ضخمة، مع دعم من الموارد البشرية الوطنية التي أصبح الملف السيبراني على قائمة الأولويات بعد أن ثبت لها أن مشروعها النووي (الذي تعوّل عليه) لا يمكن أن يحقق أهدافه دون وجود حصانة رقمية راسخة.

يضاف الى كل هذه المسائل، السمة الفريدة لفضاء الفيض السيبراني الذي يمكن أن يتيح لإيران فرصة تهديد ومهاجمة أهداف استراتيجية لخصومها التقليديين بكلف قليلة، وضمن ساحة نزاع تتجاوز عقبة توازن القوى التقليدية الذي حال دون قدرتها على الرد ضد الضغوط التي مارستها الولايات المتحدة الأمريكية، وحلفاؤها، على النظام، مع غياب قدرته على ممارسة ردع عسكري مناسب.

لقد تولد حضور خطاطة من نمط جديد في إيران نتيجة حرص النظام على قرن مسألة الحضور السيبراني، وبكافة تفاصيله، مع مصير الثورة الإسلامية، والحفاظ على جميع مكتسباتها العقدية، والتقنية، والأمنية، والعسكرية. ورغم أن تعميم هذه التعالقات لم يكن صائباً في جميع جوانبه، فإن هذه الفوبيا قد ولّدت مناخاً خدم إيران على صعيد تطوير قدراتها السيبرانية، بشكل غير مسبوق، وخلال بعد زمني قصير، بحيث تطوّر حضورها الى إعصار رقمي هادر بات يقلق الجميع بعد أن بلغت رياحه العاصفة الكثير من سواحل المحيط السيبراني لبلدان كانت تعد محيطها السيبراني بمأمن تام من مثل هذه العواصف التي لم تكن لها بصمة على الخرائط الجغرافية للتهديدات المحتملة.

وشأن بقية المجتمعات الملتحقة بفضاء الفيض السيبراني ظهرت ممارسة عمليات القرصنة السيبرانية بوصفها سلوكاً فردياً حاول بعض المستخدمين بواسطته، البرهنة على قدراتهم السيبرانية المتميزة، وجدارتهم في اختراق مواقع الغير. وتطورت القرصنة من هواية الى حرفة احترفها البعض لتهديد كيانات رقمية، أو التسبب في توقف مواقع تعود الى شخص نستبطن له العداوة، أو شركة منافسة نسعى الى التغلب عليها بطريق غير مشروع.

وأسهمت جدران الحظر التي أرساها النظام، وترويجه لعمليات الكف السيبراني التي مورست للتضييق على المعارضة في تثوير مهارات القرصنة السيبرانية كخيار حتمي لتجاوز الحظر والانفتاح على الفضاء العولمي، فتحولت إيران الى بيئة مناسبة لاستنبات جيل عريض من قراصنة المعلومات، الذين مارسوا القرصنة بنطاق واسع، وبدأت الكثير من مجاميعهم بالعمل مع النظام، بصورة مباشرة أو غير مباشرة، والتنسيق في شن هجمات على مواقع المعارضة بالدخال وخصوم إيران بالخارج.

ولم تكن الاختراقات، أو التهديدات التي مارسها قراصنة المعلومات الإيرانيين، قبل أحداث عام 2009، ترقى الى مستوى الهجمات المنسقة، بل كانت عبارة عن ردة فعل آنية تنشب نتيجة للإحساس بوجود ممارسة رقمية تسيء الى الأمة الإيرانية، أو منظومتها العقدية، أو تسعى الى الانتقاص من عمقها الحضاري الموغل بالقدم في الطبقات الجيولوجية العميقة للتاريخ الإنساني.
بيد انها بدأت تنصبغ شيئاً فشيئاً بصبغة سياسية، نتيجة لسعي الإدارة الحكومية المحموم في تجنيد جحافل من القرصنة الشباب للعمل ضمن آلتها السيبرانية من جهة، ولاستشعار بعض الفئات التي تمارس القرصنة بوجود تحرّك عولمي لتهديد الاستقرار وإشاعة الفوضى بالبلاد، فالتحقوا بصورة مباشرة، أو غير مباشرة في أنشطة قرصنة ـ بدائية

ذات صبغة دفاعية، لدرء المخاطر والتهديدات المحتملة على المواقع الإيرانية المنتشرة في فضاء الإنترنيت، أو لحظر أو تشويش بعض المواقع الإخبارية الأجنبية، ومواقع المعارضة الإيرانية لكف خطابها المناهض للنظام.

وأسهمت الهجمة الشرسة لفايروس *Stuxnet* والتي امتدت بين عامي 2009 و2010، (وأحدثت تدميراً في منشآت إنتاج اليورانيوم المنشط بلغت نسبته حوالي 20%) في إحداث صحوة إيرانية، ونهضة سريعة بعد أن عمدت الإدارة الحكومية في ولاية روحاني بزيادة كبيرة في حجم التخصيصات المالية المخصصة للارتقاء بقدرات إيران الدفاعية والهجومية، على صعيد الموارد المادية والبشرية على حد سواء، بحيث عدّ خبراء المعهد الإسرائيلي لدراسات الأمن السيبراني *INSS* أن التهديدات التي ستصاحب هذه النهضة السيبرانية ستكون أشد خطورة من التهديد النووي المحتمل عن تطور قدراتها التقنية في هذا المضمار (*INSS,2015*).

حيث شهدت المرحلة التي تلت هذه الهجمة الفريدة، حراكاً استثنائياً، وبدأنا نتلمس وفاقاً غير معلن بين كثير من الفصائل السيبرانية، وقراصنة المعلومات الإيرانيين، بالإضافة الى تنامي النزعة الوطنية لدى المستخدمين الإيرانيين، والذين وجدوا في هذه الهجمة تهديداً للإنجازات التي يحققها المواطن الإيراني، وبصرف النظر عن انتماءاته وولاءاته العقدية والسياسية، فهبّ الجميع لدرء الخطر السيبراني المحدق بالبلاد، ولم تمرّ سوى بضعة شهور على المصاب حتى بدأنا نشهد توجهات سريعة، نحو تطوير القدرات الدفاعية، مع البدء بإرساء أسس متينة لقوة ردع رقمية لم تكن مدرجة ببرامج وحسابات ال نظام، والتي صبّت نتائجها في مصلحة وتوجهات مؤسسة الحرس الثوري الإيراني، ودعوته المستديمة لتطوير قوة الردع السيبراني لإيران.

وشأن برنامجها النووي (الذي لا زال الغموض يلفه من نواح كثيرة، ولم تفلح الدول الكبرى في كشف النقاب عن جميع تفاصيله التي لا زالت إيران تحتفظ بالكثير من خيوطها المتشابكة) حرصت إيران على إنشاء هيكلة لمؤسسات الدفاع وحروب المعلومات اتصفت بتعقيد كبير، مع تعدد طبقات إداراته، وتشابك العلاقات الرابطة بين فصائله، ووحداته الدفاعية والضاربة، بالإضافة الى نشر حضور هذه المؤسسات ضمن أكثر من بقعة، ضمن الإدارات الحكومية المدنية، والأمنية والعسكرية بحيث تورث خصومها السيبرانيين عقبة تتبع موارد هجماته المحتملة، أو بلوغ مستوى مقبول لتقدير حجم سلطانه السيبراني في الفضاء السيبراني الافتراضي.

لقد توغلت هيمنة النظام الإيراني، خلال العقود الثلاثة الأخيرة، فبلغ سلطانها الى أعماق سحيقة في منظومة إدارة ومراقبة نظم الاتصالات والمعلومات المحلية، كما أن تعدد مسارات تعاملها، مع مختلف قطاعات هذا النشاط، منذ دخول فضاء خدمات الإنترنيت الى البلاد، وتعدد أشكال الهيكلة المؤسساتية التي سعت الى تشكيلها، وتعدد المراجعات لبنية هذه المؤسسات، للتأكد من نجاح الاستراتيجية الأمنية، وارتفاع مستويات الحصانة، نتيجة الى السعي المستمر لتشتيت مراكز القوى، والمبالغة في تشبيك العلاقات الرابطة عن عناصر هذه المؤسسات، وتغييب دور الإدارات بشكل متعمد، الأمر الذي مهد للنظام فرصة إشراك عدد كبير من قطّان الفضاء السيبراني وخبراء تقنياته، ومن مختلف قطاعات الأنشطة السائدة في المجتمع الإيراني، ضمن مصفوفة معقدة، تضم عدداً هائلاً من المهام، وبتراتبية لا يمتلك المفتاح السحري لربط عناصرها المتوزعة، وتحويلها الى خطاطة أمنية راسخة إلا صفوة من قيادات النظام التي تتوزع

بين قمة الهرم الحكومي، ومؤسسة الحرس الثوري الإيراني، والباسيج، وبإشراف مباشر من قبل المرشد الأعلى للثورة الإسلامية.

من أجل هذا لن نجرؤ على الادعاء إن تحليلنا لهذه الهيكلة المعقدة سينجح بصورة تامة في وصف هوية ومهام هذه البنى المؤسسية، أو أن عملية تشخيص العلاقات القائمة بين هذه الكيانات، وأسلوب صناعة القرارات ووضعها حيز التنفيذ ستأتي متطابقاً مع تشعبات العلاقات الرابطة بين هذه العناصر المتكاثرة والمتداخلة بالوقت ذاته (*Wheeler,2013*).

لقد نجحت إيران في أن تستأثر لنفسها موطأ قدم على ساحة المنازلة والمجالدة السيبرانية العولمية، والتي لم تفلح بالحضور فيها إلا دول متقدمة تمتلك ناصية التقنية السيبرانية مثل الولايات المتحدة، وروسيا، والصين، وإسرائيل. وانتقلت خلال بعد زمني قصير، لم يتجاوز بضع سنوات، ونجحت في التحوّل من ممارسة تهديدات محدودة، وهجمات بدائية على بعض مواقع الويب غير الحصينة (التي تعود لمستخدمين يستوطنون دائرة المعارضين، أو شركات منافسة) الى شنّ هجمات تتسم بنهج بالغ التعقيد، مع حضور تنسيق عال بين الفصائل السيبرانية المشاركة في تنفيذها من داخل إيران وخارجها.

ولا يمكن أن يعد التطور في السطوة السيبرانية الإيرانية مصدر قلق لدول المنطقة، أو لبقية دول العالم لو عمدت الى توظيف نتائجه في ترسيخ حضورها في مجتمع المعرفة العولمي، أو فتحت آفاق جديدة للتنمية من خلال الدخول الى ميدان اقتصاد المعلومات والمعرفة، وغيرها من النشاطات التي كانت ستنعكس على التنمية الاقتصادية والمعرفية في البلاد، ولكنها على النقيض من ذلك فقد سعت للظفر بهذه القدرات الغاشمة لتحقيق غايات تستبطن نزعات سياسية وأخرى عقدية لضمان بسط نفوذها في المنطقة، وبسط سلطان ثورتها الثقافية على بلدان قد لا تميل نحو الانصياع لخطاطة النظام الإيراني.

وقد انتهزت إيران فرصة انشغال الولايات المتحدة الأمريكية، ودول العالم التي ساهمت معها بالمباحثات المعقدة حول برنامجها النووي، لتمرير مشروعها الأشد تعقيداً، والذي يقيم في فضاء متخيّل، يصعب تحديد حجم القدرات المستبطنة في كياناته السيبرانية، أو تحديد حجم الفصائل السيبرانية المشاركة بأنشطته، أو تحديد هوية المشاركين في التهديدات التي قد تنبع من تربته التي تتصف عناصرها بتعقيد يفوق الى حد كبير التعقيدات المنبثة في ساحة الملف النووي ذاته، فطوّرت آلة الدفاع لديها، قبل أن تتوجه نحو تطوير آلة ردع رقمي غاشمة، وعزّزت برنامجها السيبراني بتهيئة كوادر تمتلك خبرات عميقة في ميدان تقنية المعلومات والاتصالات، ولملمت شمل قراصنة المعلومات المحليين، وجمعت فصائلهم تحت مظلة ميليشيات رقمية ربطت عملها بمنظمة الباسيج، ومؤسسة الحرس الثوري الإيراني، ثم عمدت الى جمع شتات مؤسساتها السيبرانية الحكومية، تحت راية المجلس الأعلى لالفضاء السيبراني الإيراني، لكي تنتظم الجهود تحت راية واحدة ولتحقيق أهداف محددة[3].

---

[3] . أسس المجلس الأعلى لالفضاء السيبراني الإيراني، برنامجاً للدفاع السيبراني في جامعة الإمام الحسين بطهران، وأنشأ مجموعة مراكز تقنية لإنتاج برمجيات مكافحة الديدان الخبيثة *Anti-Malware* التي تنتج في إيران، مع التوجه نحو تحليل المعمارية البرمجية للديدان الخبيثة التي تنتشر في الفضاء السيبراني للانترنيت، والتي أنشئت لاختراق الفضاء السيبراني الإيراني، ولإحداث تأثيرات ضارة على مختلف أشكال كياناته السيبرانية. كما شجعت هذه المراكز وبالتنسيق مع المؤسسات الأكاديمية على إعداد برامج تدريبية، ذات طابع أمني، لنشر الوعي الأمني لدى مستخدمي الإنترنيت، والارتقاء بالمهارات والقدرات لدى كوادر المؤسسات الحكومية والقطاع الخاص على صعيد تمتين الحصانة الأمنية لشبكات المعلومات، ومكافحة الهجمات التي تمارس عليها بواسطة الفايروسات الحاسوبية والديدان الخبيثة (*Schwarz,2013*).

كما لم يقف طموحها عند هذا الأمر فتوجهت نحو إنشاء بؤر رقمية في البلدان العربية التي تحتضن صراعات إقليمية أو عولمية، مثل: لبنان، وسورية، وغزة، واليمن، فاستنبتت فيها وكلاء رقميين، تجمعها بهم توجهات سياسية أو عقدية مناوئة لخصومها التقليديين، وعززت قدراتهم بما يبسط سلطانها، ويسهم في تمديد أذرع تأثيرها، مع استبقاء النظام بعيداً عن الأنظار، وإلصاق بصمة النشاط بوكلاء رقميين لا ينتمون الى الهوية الإيرانية.

ونتيجة لهذا التوسع الشبكاتي، الذي يتسم بمعمارية بالغة التعقيد، ولكثرة الكيانات المشاركة في هذا المشروع السيبراني الطموح، ولتداخل المصالح وتكاثر الأسباب والعلل، أصبح من الصعوبة بمكان تحديد بدايات شروع التهديد أو الهجمة، أو مكانها، أو تشخيص غاياتها، أو هوية المساهمين فيها، الأمر الذي بات يشكل تهديداً حقيقياً لدول كبرى مثل الولايات المتحدة، وبريطانيا، وإسرائيل، والتي تعد كياناتها السيبرانية على أولويات قائمة الأهداف التي يروم النظام الإيراني الوصول إليها.

خامرتني فكرة هذا الكتاب ضمن محور أشد اتساعاً يعنى بمسألة النزاعات السيبرانية وتوازن القوى اللينة على المستوى العولمي. وسعيت الى إنضاجها حتى وجدتني مساقاً الى مجال أشد اتساعاً من مجال فضاء الفيض السيبراني الذي احتوى جميع تفاصيل حياتنا المعاصرة. فانصرفت عن الكتابة لوهلة من الزمن قبل أن أعاود التفكير في انتخاب جزء مهم من ساحة المجالدة السيبرانية فلم أجد أفضل من ساحة النزاع المستتر في الفضاء السيبراني الإيراني. فالتجربة الإيرانية التي حاولنا أن نخضعها للحفر والدراسة والمباحثة، هي واحدة من المسائل القلائل التي لا تكاد تعثر على دراسة مستفيضة في المكتبة العربية، أو كتاب في المكتبة العولمية قد صبّ اهتمامه على مسألة السطوة السيبرانية الإيرانية، لاستشراف تداعياتها المستقبلية على فضاء الفيض السيبراني في منطقة الشرق الأوسط، وفرص توسعها وانتشارها على مساحة واسعة من الفضاء السيبراني العولمي، الذي تستوطن فيه الكثير من الكيانات السيبرانية التي تعود الى خصوم إيران على المستوى السياسي، أو العقدي.

وإن كان البعض يعتقد أن الملف النووي الإيراني يعد من أعقد الملفات المطروحة على طاولة السياسة خلال العقد الأول من الألفية الجديدة، فإن هذا الاعتقاد سيتزعزع لا محالة بعد مراجعة الحقائق وتفاصيل الملف السيبراني الإيراني الذي تحفّه عقبات من نمط جديد، مع غياب استراتيجية دولية للتعامل مع التهديدات السيبرانية وعدم نضوج المعالجات التي عنيت بمسألة أمن فضاء الفيض السيبراني، إذا ما قورنت بالتراث والنضوج الذي تتمتع بها مسألة التقنية النووية وتطبيقاتها المختلفة.

لقد ارتسمنا لأنفسنا، منذ البداية، هدفاً مخصوصاً حددنا ملامحه بممارسة الرصد التقني المحايد، والاستكشاف الذي يسترشد بخطاطة الأمن السيبراني، والتزمنا به أثناء ممارسة عمليات التنقيب والتحري داخل حدود فضاء إيران السيبراني. بلّ قدّرنا أن تحليل مادة المحيط السيبراني الإيراني، وتوصيف وقائع السجالات الدائرة في مجاله، سيكون إسهاماً في معالجة موضوع جديد، وشائك، بالوقت ذاته، بمقاربة موضوعية ستسهم في إلقاء الضوء على ملف مهم لم يقع ضمن اهتمامات صنّاع القرار في وطننا العربي، وهو بالوقت ذاته، امتثال لدواعي المعالجة المعرفية التي سيستوي على قواعدها بناء أسس راسخة لأمن معلوماتي عربي متين.

وبذلنا كل ما في وسعنا خلال فصول هذا الكتاب (الستة)، استدعاء، ومراجعة، وتحليل جلّ تفاصيل مشهد الحضور السيبراني الإيراني في فضاء الفيض السيبراني، وسعينا الى فهم عناصر سطوتها السيبرانية المتنامية خلال العقدين الأخيرين، بعيداً عن النهج المتشنج الذي ساد في دراسة تفاصيل المشهد الإيراني، لكي نفلح في تفكيك جميع عناصر المشهد السيبراني الإيراني، ونقف على الأسباب الكامنة وراء هذا التطور السريع، ولكي تكون هذه الدراسة مدخلاً يمكن أن نلج من خلاله الى بوابة لتطوير القدرات السيبرانية لمجتمعنا العربي، ويؤمن لنا بالوقت ذاته، فرصة بناء كفاية أمنية عربية، قادرة على درء المخاطر، التي باتت تهدد عصر مجتمع المعرفة، الذي تعيش مرحلة بداياته الكثير من دولنا العربية.

لم نشأ أن نكرّس الكتاب لمساجلة بين هذا المعسكر أو ذاك، فتدفعنا صبغة الانتماء لأحدهما الى محاولة تشويه بعض عناصر المشهد لترجيح كفة المعسكر الذي ننتمي إليه على حساب المعسكر الآخر، متوهمين أن مخالفة الواقع يمكن أن تصطنع تفوقاً، أو تبني سطوة لا وجود فيها إلا في خيالاتنا المتهافتة. وإنما أردناه أن يكون مساحة للتعبير بموضوعية عن واقع يمكن أن يشعرنا بحجم التراجع التقني الذي نعيشه في ميدان الأمن والكفاية السيبرانية في عموم بلداننا العربية.

من أجل هذا وجدنا لزاماً علينا هجران النهج السائد في هذه الأيام، والذي يحرص على تصعيد النزاع مع الآخر وتشويش المشهد الذي يربطنا ببعض مساحاته، بدلاً من الدراسة الموضوعية والمحايدة التي تسهم بفهم أكثر عمقاً بعناصر سطوته أو تفوقه في هذا المضمار أو ذاك، بعيداً عن الترتيبات الأيديولوجية التي تعتبره منطقة محرمة، ولا تصلح سوى لعمليات النقد والاستهداف التي تجرنا في كثير من الأحيان الى عدم القدرة على وضعه في المكان الصحيح. بالمقابل سعينا الى ممارسة عملية تفكيك محايد وموضوعي، لتشخيص مواطن القوة لديه، على التوازي مع تحديد هوية وحجم التناقضات والمشكلات التي تسود في المحيط السيبراني الإيراني، بقصد تجاوزها في محيطنا السيبراني العربي الذي لا زالت مسألة الأمن السيبراني غائبة عن مشهده في عموم بلدان وطننا الكبير.

ويمكننا القول أن هذه الدراسة قد ولدت في فضاء معرفي يحفل بتحديات غير تقليدية. فمحاولة دراسة رقعة رقمية، في الجغرافية غير المتعينّة لفضاء الفيض المعلومات، تشكل عقبة كبيرة بسبب اتساع رقعة الالفضاء السيبرانيي وعدم وضوح حدودها، وطبيعة تضاريسها الجغرافية. يضاف الى ذلك العقبة التي تنشأ عن شحة المعلومات عن الفضاء السيبراني الإيراني، الذي يحرص النظام الإيراني على استبعاده عن أنظار خصومه الذين يحاولون استغلال أي فجوة لتوظيفها في عملية الاختراق السيبراني، وممارسة الضغوط على فضائها السياسي والعقدي، وبرنامجها النووي، وبرامج التسلّح، وغيرها من البرامج الطموحة في منطقة الشرق الأوسط المشحونة بالأزمات والتشنجات السياسية.

ومما زاد المشهد تعقيداً هو عدم وضوح مفهوم السطوة السيبرانية، وتباين الآراء بصدد تحديد مفهوم حروب فضاء الفيض السيبراني، وغياب القدرة على تمييز هوية المساهمين في التهديدات والهجمات السيبرانية بسبب عدم وضوح الهوية السيبرانية في فضاء مفتوح مع وجود أكثر من فرصة لتغييب الحضور، أو تشويش الهوية من خلال افتعال هويات مزيفة وأخرى مموّهة *Avatars* يصعب الكشف عن انتماءاتها لهذه الرقعة الجغرافية، أو الكيان السياسي، أو ذاك.

وأخيراً تشخص أمامنا الهوية الإيرانية، التي تتسم بسمات فريدة، فنزعتها نحو التحرر من القيود التي يفرضها النظام، وحرصها على القفز من فوق العقبات التي يرسيها النظام في الفضاء السيبراني الوطني، تغيب فجأة وتتحول الى نزعة

وطنية تمتلك عمقاً بعمق الحضارة الفارسية الموغلة بالقدم، فينقلا المواطن من معارض عنيد، الى موال لا تبصر عينيه سوى مصالح إيران، بصرف النظر عن التوافق أو التناقض الصريح في الأهداف، أو المصالح، أو التوجهات السياسية.

وحاولنا أن نعوّل في إنجاز هذا العمل على مدوّنة واسعة تنتمي نصوصها الى حقول متنوعة تلتحق بمجالات رقمنة الواقع، وفضاء الفيض السيبراني المتخيَل، والسطوة السيبرانية.

وقد كلفنا الحصول على هذه الموارد، وتحليل مادتها الكثير من الوقت والجهد، في نسيج تسوده فجوات في أحيان، أو تغلفه توجهات النظام الإيراني في تشويش المشهد، وتغييب بصمات الجهات التي تساهم في تشكيل هذا المشهد، أو ذاك.

وحرصنا على أن ندوّن جل ما رصدناه من أمارات توثق بدايات ومآلات الإعصار السيبراني الإيراني، وإذ نقوم بذلك، ذلك من حيث أننا معنيّون بمسائل الجاهزية والكفاية الأمنية لبنى المعلومات والاتصالات ـ التحتية في وطننا العربي، بوصفها مجالاً من مجالات الأمن السيبراني العربي، لأن المشهد العربي العام بات يحملنا على الاقتناع بضرورة استنبات وعي أمني ـ رقمي من نمط جديد، ويحتم علينا المساهمة في تسارع تجلياته في حضرة التصاعد غير المسبوق للتهديدات والهجمات السيبرانية المتلاحقة، والتي تحصل على التوازي مع توسع رقعة مجتمعات المعلومات والمعرفة في عموم بلداننا العربية، وانغماس المواطن العربي بالتطبيقات السيبرانية التي باتت تشدّه الى أعماق سحيقة في فضاء الفيض السيبراني المفتوح، دون أن تنهض لديه وعياً كافياً بطبيعة وحجم المخاطر المحتملة عن هذا التوغل السيبراني في جميع مفاصل حياتنا اليومية.

وعند هذا المشهد المشحون التهديدات والمخاطر السيبرانية، نريد أن نقف وقوف التأني، لا بالانخراط في تحليل بعيد عن الأسس العلمية والموضوعية، وإنما بالتشخيص العارف الذي يسعى الى تعقل جميع تفاصيل المشهد، وتفاصيل تداعياته المـ حتملة، لينتج من قراءة تجارب الآخر، بإخفاقاتها ونجاحاتها مشهداً جديداً يمكن أن نوظّب فيه جميع مواقع كياناتنا السيبرانية، والوصلات التشعبية الرابطة بينها في حضور رقمي عربي، آمن ورشيد. ولا يمكن أن يتحقق ذلك إلا من خلال دراسات لاحقة تولي بالعناية جميع تفاصيل الكفاية الأمنية للحضور السيبراني العربي في فضاء الفيض السيبراني العربي، بدلاً من تضخيم حجم الثمار التي نجحنا في استنباتها، أو التقليل من شأن ما أنجزه الآخر والسعي الى الانتقاص منه بشتى الطرق لإثبات وهم تفوقنا الذي لا زلنا نكابر به رغم كثرة العثرات التي تعرضنا له، وضخامة حجم الإخفاقات وخيبة الأمل التي منينا بها بعد آخر صحوة ترافقت مع الربيع العربي الذي لم يفلح في إحداث ما كانا نأمل بتحقيقه، ونوال ثماره المتخيّلة.......

إن هذا الكتاب يمكن أن يعد دعوة الى ثلاثة مطالب: بيان حجم السطوة السيبرانية التي نجحت إيران ببلوغها، ومحاولة الكشف عن بعض الجوانب الرشيدة من الاستراتيجية التي تبنتها إيران لتطوير قدرات الدفاع والردع السيبراني بحيث أضحت تتبوأ بجدارة المرتبة الرابعة بين الجيوش السيبرانية لكل من الولايات المتحدة، وروسيا،

والصين، وتتفوق على دول تتفوق عليها تقنياً وعسكرياً. وأخيراً التأكيد على ضرورة البدء بتفكير حقيقي في واقع الكفاية الأمنية للنسيج الشبكاتي للدول العربية، وكيفية النهوض به بحيث نكون قادرين خلال عقد من الزمان على درء مخاطر التهديدات والهجمات السيبرانية التي بدأت تطرق بوابات فضاء بلداننا، وأحدثت بعضها تأثيرات ضارة وموجعة في كيانات رقمية تنتمي الى مؤسسات حكومية، وأخرى تخص قطاع إنتاج النفط والغاز، وقطاعات التجارة والأعمال.

حسن مظفر الرزو
مستشار لشؤون التخطيط الاستراتيجي
الموصل، العراق
2020

الفصل الأول:
خصائص مجتمع المعلومات الإيراني وخصائص نسيجه السيبراني

الفصل الأول: خصائص مجتمع المعلومات الإيراني وخصائص نسيجه السيبراني

1 . مجتمع المعلومات في إيران: مقدمة تمهيدية:

يعد مجتمع المعلومات من التراكيب المجتمعاتية التي تعتمد في ديمومة بقاءها على إنتاج، ونشر، وتوزيع، واستخدام، وتكامل، ومعالجة محتوى مادة البيانات، وتسعى الى استثمار حصيلة هذه العمليات والمعالجات في إدارة أنشطتها بقطاعات الاقتصاد، والسياسة، والثقافة.

وتعد تقنية المعلومات والاتصالات، واداوتها السيبرانية الأداة الأساسية لتسيير دفة الأنشطة السائدة في مجتمع المعلومات، والتي تعتمد في ترسيخ حضورها على وفرة بنية تحتية ـ متماسكة قادرة على احتضان الفيض السيبراني للمعلومات الذي تنتجه أنشطة المجتمع الجديد، أو تتواصل مع مادته السيبرانية مع مجتمع المعلومات العولمي الذي بات يلف كرتنا الأرضية من جميع الاتجاهات.

ولما كانت عملية الانتقال من المجتمع الصناعي نحو عتبة مجتمع المعلومات، تدريجية، ومتداخلة (مع كثير من عناصر حضور هاتين المرحلتين) أصبحت عملية تحديد مستوى انتماء مجتمع من المجتمعات الى مجتمع المعلومات، أو تطوره باتجاه مجتمع المعرفة، عملية صعبة، تحفّها الكثير من العقبات المفاهيمية.

من أجل هذا سعت المنظمات الدولية، (التي تعنى بتحديد مستويات انتماء المجتمعات المعاصرة الى خطاطة مجتمع المعلومات) الى اقتراح مجموعة من المعايير والمؤشرات التي يمكن الاسترشاد بها في تحديد التحاق المجتمع او غياب حضوره عن بيئة مجتمع المعلومات المعاصر.

وسنحاول أثناء محاولتنا لدراسة معالم التحوّل نحو مجتمع المعلومات في إيران، بيان مستوى نضوج هذه المرحلة الانتقالية، وهل أن التحوّل لا زال في بداياته أم أنه قد حقق مراحل متقدمة على صعيد الالتحاق بخطاطة المجتمع الجديد. وسنحاول (في الوقت ذاته) تتبع مستويات تغلغل عملية التحول في عموم نسيج المجتمع الإيراني، وبناه التحتية الممتدة على عموم الرقعة السكانية، والجغرافية للبلاد بقصد تحديد فيما إذا كانت عملية التحوّل كلية، أم انها عبارة عن تحول ونمو مطرد في مساحات محدودة، مع تكاثر الفجوات في مساحات شاسعة من نسيج المجتمع، وعدم تناسق عمليات التحوّل نتيجة لتذبذب توجهات إدارات المنظومة العقدية والسياسية التي تتشابك خيوط خطاطاتها المنتجة للمشهد الذي يبزغ على سطح الواقع الإيراني في وقتنا الراهن.

2 . خصائص البيئة الحاضنة لمجتمع المعلومات الإيراني:

تتألف البيئة الحاضنة لمجتمع المعلومات في إيران من بنية تحتية داعمة يتألف نسيجها من شبكات المعلومات والاتصالات التي يسري فيها الفيض السيبراني لفضاء معلومات الشبكات المحلية وبيئة الانترنيت. ويقيم في مجال هذه البيئة الحاضنة مجموعة من الأدوات التي تدعمها حزمة من التطبيقات التي تسهم بتسيير دفة الأنشطة التي تسود المجتمع السيبراني الإيراني، شأن بقية مجتمعات المعلومات والمعرفة المعاصرة.

وفي خضم هذا النسيج الشبكاتي المعقد يبرز دور الموارد البشرية التي تتفاعل مع حضور هذه الأدوات وتستثمرها في إدارة دفة أنشطة المجتمع وترسيخ هوية بصمته الوطنية في أسلوب التعامل مع هذه الأدوات، وتوظيفها لإنتاج كيان

متخيل لمجتمع من نمط جديد يستوطن الفضاء السيبراني المتخيّل السيبراني، وبنسخة رقمية موازية لحضور المجتمع التقليدي.

2 . 1 . البنية التحتية للمعلومات والاتصالات:

تحوّل نهج الحكومة الإيرانية خلال السنوات التي تلت عام 2006 باتجاه ترسيخ الاهتمام بالبنية التحتية للمعلومات والاتصالات، بعد أن سخّرت حجماً كبيراً من النفقات لتحقيق هذه الغاية على حساب قطاع توفير الخدمات، وبنسبة ناهزت 6 : 1. وبالوقت ذاته ارتفعت حصة المواطن من التخصيصات المالية الوطنية لقطاع المعلومات والاتصالات، خلال السنوات 2002-2010 من 1.26 دولاراً الى 10.51 دولاراً[4] (*Soofi&Ghazinoory,2013*).

وقد نجح هذا التوجه في ضمان امتلاك إيران لبنية تحتية عملاقة من شبكات الاتصال الهاتفي (الأرضي والمحمول) والألياف البصرية التي قد تغلغلت في عموم رقعتها الجغرافية.

2 . 1 . 1 . شبكات الهواتف الأرضية والمحمولة:

تمتلك إيران شبكة هاتفية أرضية تغطي 77 % من القرى المنتشرة في عموم البلاد، حيث يستثمر هذه الخدمة حوالي 29.5 مليون مشترك، وبنسبة اشتراك تبلغ حوالي 37 %. بينما تتفوق عليها خدمة الهاتف المحمول التي تغطي شبكاتها حوالي 94.2 % من عموم البلاد، وبعدد مستخدمين تجاوز 71 مليون مشترك، وبنسبة اشتراك بلغت حوالي 91 % ـ أنظر الجدول (1 - 1) (*M.o.ICT,2015*).

الجدول (1 - 1) ـ انتشار خدمات الهواتف الأرضية والمحمولة في إيران، عام 2015.

المتغير	الهواتف الأرضية	الهواتف المحمولة
أعداد المشتركين بالخدمة الهاتفية.	29,417,318	71,142,411
نسبة المشتركين بالخدمة الهاتفية.	37.7 %	91.0 %
نسبة التغطية التي توفرها الشبكات الهاتفية.	% 77.0	94.2 %

المصدر: (*M.o.ICT,2015*)

ومن بين حوالي 22.8 مليون مسكن تنتشر على عموم الرقعة الجغرافية لإيران، نجد حوالي 97.6 % منها مرتبطاً بالخدمة الهاتفية الأرضية، أو المحمولة، أو كلاهما. وتتوزع هذه النسبة الى 98.9 % في مراكز المدن، 93.9 % في المناطق الريفية. ويتمتع حوالي 54.0 % من سكان المساكن بخدمة الانترنيت، حيث تتوزع النسبة الى 45.1 % بالمسكن المنتشرة بالمناطق الحضرية، و17.5 % بالمساكن المنتشرة في المناطق الريفية (*M.o.ICT,2015*).

وتتوفر خدمة الجيل الثالث للمحمول لحوالي 52 % من المشتركين المرتبطين بشبكة الهواتف المحمولة، بينما تتوفر خدمة الهواتف الأرضية المحمولة، لتلبية الاحتياجات الآنية للمواطنين بعموم البلاد من خلال 152,758 خط فعال (*M.o.ICT,2015*).

[4] . بيد أن مضاعفة حصة المواطن الإيراني لا تكاد تشكّل رقماً قياسياً إذا ما قورنت بالدول المتقدمة التي قد يبلغ تخصيصها لحصة المواطن من تطوير تقنية المعلومات والاتصالات حوالي 2000 دولاراً.

تهيمن المؤسسة الحكومية على تشغيل شبكات الخطوط الهاتفية ـ الأرضية في البلاد، حيث تنهض بهذه المهمة شركة إيران للاتصالات *TCI*. بالمقابل تتوفر خمس شركات لتشغيل شبكات الهاتف المحمول في عموم الرقعة الجغرافية للبلاد ـ أنظر الجدول (1 - 2).

الجدول (1 - 2) ـ أهم الشركات الإيرانية التي تشرف على تشغيل شبكات الهاتفية بالبلاد.

الشركة	مجال التشغيل
شركة *TCI (PTT)*.	شبكة هواتف محمولة
شركة إيران للاتصالات *TCI*.	شبكة هواتف أرضية.
شركة *MTN Irancell*.	شبكة هواتف محمولة
شركة *TRI* أصفهان.	شبكة هواتف محمولة
شركة *Kish* للاتصالات.	شبكة هواتف محمولة
شركة *Taliya*.	شبكة هواتف محمولة

في بداية عام 2007، أعلنت شركة الاتصالات الإيرانية *TCI* أن عدد المشتركين بخدمة الهاتف المحمول قد تفوق على أعداد المشتركين بخدمة الهواتف الأرضية. وقد هيمنت شركة *MTN* على نسبة 68 % من أعداد المستخدمين، بينما جاءت بالمرتبة الثانية شركة *IranCell*، ثم شركة *Taliya* بالمرتبة الثالثة. وتوجد شركات أخرى مثل: *Kish Company*، و *Mobile Telecommunication Company of Esfahan* (*Abbasi, et.,al.,2008*).

تنهض شركة إيران للبنية التحتية (التي ترتبط مباشرة بوزارة الاتصالات والمعلومات) بمهمة تجهيز الخدمة الهاتفية ـ الدولية لعموم المشتركين في البلاد. وتتوفر أكثر من وصلة اتصال لشبكة الخطوط الهاتفية الإيرانية بفضاء الاتصال العولمي بلغ عديدها أربع وصلات هي (*Wikipedia,2015*):

- ✓ الوصلة الأولى: القابلو المحوري البحري للألياف البصرية المرتبط بدولة الامارات العربية المتحدة، والمتصل بشبكة الألياف البصرية العولمية *FLAG*.
- ✓ الوصلة الثانية: القابلو المحوري العابر لمنطقة آسيا ـ أوربا *TAE* والذي يسافر من أذربيجان عبر المناطق الشمالية من إيران باتجاه تركمنستان، والتوسعة باتجاه جورجيا وأذربيجان.
- ✓ الوصلة الثالثة: خط راديوي *HF* وخط الموجات الميكروية المرتبط مع تركيا، وأذربيجان، وباكستان، وأفغانستان، وتركمنستان، وسورية، والكويت، وطاجيكستان، واوزبكستان.
- ✓ الوصلة الرابعة: المحطات الأرضية للأقمار الصناعية (*9 Intelsat+ 4 Inmarsat*).

بالإضافة الى هذه الوصلات الاتصالية فقد قامت إيران بمد قناة ألياف بصرية مع قابلو شبكة اتصالات بحرية في الخليج العربي، تمهيداً لربط البلاد بشبكات الألياف البصرية العولمية عبر الحدود الشمالية ـ الغربية للبلاد.



بقيت شركة الاتصالات الايرانية *TCI* المجهز الحصري (الحكومي) لخدمات الهواتف الأرضية والمحمولة في عموم إيران لحين منح ترخيص شركة *GSM* للهواتف المحمولة الى شركة *Turkcell* التركية.

وتهيمن شركة إيران لإنتاج الهواتف على سوق تجهيز الهواتف في عموم البلاد. وقد حصلت هذه الشركة على اتفاقية ترخيص مع شركتين، إحداهما: الفرنسية *Al-catel-Sel*، والثانية: الألمانية *Siemens*. وقد تقاسمت الشركة الإيرانية مع هاتين الشركتين، وبمشاركة مباشرة من المصرف الصناعي (بلغت حصة *TCI* 45 %، وحصة المصرف الصناعي 35 %، بينما تقاسمت الشركتين الفرنسية والألمانية نسبة 20%) (*EIU,2004*).

وتقوم كل من شركة إيران المتحدة للصناعات الاتصالية *Parstel* (والتي تنتج بترخيص من شركة *Daewoo* الكورية)، وشركة *Paya* (التي تنتج بترخيص من شركة *LG* الكورية) بإنتاج مجموعة متنوعة من أدوات المعلومات والاتصالات. يضاف الى ذلك وجود حضور منتجات مختلفة من شركات عالمية مثل: *Ericson*السويدية، *Nokia* الفنلندية، *Italtel* الإيطالية، في سوق أدوات المعلومات والاتصالات بإيران (*EIU,2004*).

2 . 1 . 2 . شبكات توزيع خدمة الانترنيت:

دخلت خدمة الانترنيت للمرة الأولى الى إيران، عبر بوابة مركز دراسات الفيزياء النظرية والرياضيات *IPM*، ومن خلال وصلة الارتباط مع شبكة *BITNET* نتيجة لعضوية إيران في شبكة البحوث للأكاديمية الأوربية *EARN*. كانت بداية الارتباط عبر خط منفرد (سرعته *9600 Baud*) استأجر من جامعة فيينا بالنمسا في بدايات عام 1993 فارتبطت منظومة الانترنيت بإيران مع المعايير الأوربية لتجهيز هذه الخدمة (*Abbasi, et.,al.,2008*).

وقد انطلقت رسالة البريد الالكتروني الأولى التي أعدها مدير مركز دراسات الفيزياء النظرية والرياضيات من إيران الى إدارات جامعة فيينا مثمناً الدعم الذي تم تقديمه لربط إيران بفضاء الانترنيت السيبراني.

بعد ذلك سمح للمؤسسات العلمية والأكاديمية بالوصول الى خدمة الانترنيت عبر بوابة مركز الدراسات، قبل أن ينفتح مجال الاستخدام لبقية القطاعات، والجماهير الإيرانية ومن خلال منصات مجهزي الخدمة في عموم البلاد (*Abbasi, et.,al.,2008*).

منذ أن وصلت خدمة الانترنيت الى إيران عام 1993[5] والحكومة الإيرانية تبذل كل ما في وسعها للارتقاء بالبنية التحتية للمعلومات والاتصالات التي تدعم انتشار الخدمة بالبلاد.

في بداية عام 1998 قامت وزارة تقنية المعلومات والاتصالات بتوفير حسابات الانترنيت للقطاع العام، وعموم المواطنين (*IBP,2011*). في البداية وصلت خدمة الانترنيت من الفضاء الاتصالي العولمي عبر شبكتين أساسيتين (*Wikipedia,2015*):

- الشبكة الأولى: الشبكة الهاتفية العامة *PSTN*.
- الشبكة الثانية: شبكة البيانات العامة *PDN*.

5 . فكانت الدولة الثانية بمنطقة الشرق الأوسط حصولاً على هذه الخدمة.

وتقوم الشبكة الأولى بتوفير وصلة للمستخدمين الإيرانيين بالفضاء السيبراني السيبراني من خلال مجهزي خدمة الانترنيت *ISP's* وبواسطة شبكة من الخطوط السيبرانية. أما شبكة البيانات العامة فتشرف على عملها شركة إيران لتناقل البيانات *DCI* والتي تقوم بتوفير الخدمات السيبرانية للمشتركين معها.

وبدأت شبكة الانترنيت تتغلغل تدريجياً في جميع مفاصل المجتمع الإيراني، فرسّخت حضورها في مختلف المؤسسات العامة ـ أنظر الجدول (1 - 3).

الجدول (1 - 3) ـ انتشار خدمة الانترنيت في قطاعات المؤسسات الإيرانية.

القطاع	نسبة الانتشار
المؤسسات الحكومية.	100 %
مراكز البحث والتطوير الحكومية.	100 %
المدارس والمؤسسات التربوية.	51.7 %
المؤسسات الصحية.	90.0 %
المصارف والمؤسسات المالية.	%100
مكاتب البريد.	90.4 %
المكتبات العامة.	76.2 %
التجارة والأعمال.	47.0 %
المتاحف.	63.0 %

المصدر: *ITO,2014*.

وبعد مدة بدأت بوابات الانترنيت بالانفتاح عبر مكاتب ومراكز خدمة، فبلغ عدد المكاتب الحكومية التي تجهز خدمات المعلومات والاتصالات 6,298 مكتباً، في حين بلغ مراكز المعلومات والاتصالات في عموم البلاد 10,030 مركزاً مع حلول عام 2014 ، بينما يتوفر في طهران فقط أكثر من 1,500 مقهى للانترنيت (*ITO,2014*).

بالمقابل بلغ عدد مجهزي خدمة الانترنيت *ISP* عام 2011 حوالي 1,230 مجهز خدمة، أدارت دفة أنشطتهم السيبرانية شركات إيرانية من القطاع الخاص وبدأت بطرح خدماتها السيبرانية في عموم إيراني (*IBP,2011*).

بلغت سعة الخدمة الدولية للانترنيت في إيران، عام 2015، 187Gbps جهزت لمختلف فئات مستخدمي الانترنيت بالبلاد بواسطة ثلاثة تقنيات أساسية، شملت: شبكات الهواتف الأرضية، وشبكات الهواتف المحمولة، وأبراج *Wi-Max* ـ أنظر الجدول (1 - 4).

الجدول (1 - 4) ـ تقنيات تجهيز خدمة الانترنيت في إيران، عام 2015.

التقنية	التفاصيل
عدد المشتركين بالخدمة العريضة بواسطة شبكة الهواتف الأرضية	7,574,042
عدد المشتركين بالخدمة العريضة على الهواتف المحمولة.	7,081,918
الاشتراك بخدمة أبراج *Wi-Max*.	1,212,603

المصدر: (*M.o.ICT,2015*)

وتتقارب أعداد الذين يتم تجهيزهم بخدمة الانترنيت بواسطة خدمة الهواتف الأرضية والمحمولة، حيث تراوحت أعدادهم بين 7-7.5 مليون مشترك، بينما تراجع أعداد المشتركين بخدمة أبراج *Wi-Max* الى 1.2 مليون مشترك (*M.o.ICT,2015*).

ويتمتع حوالي 44.1% من السكان بخدمة الانترنيت العريضة ـ الثابتة، بينما يتمتع 30.2 % من السكان بالخدمة العريضة ـ اللاسلكية، بينما يتمتع 9.7 % من السكان بخدمة موجة ضيقة، ويتمتع حوالي 9.8 % بخدمة محمولة ـ ضيِّقة (*M.o.ICT,2015*).

بالمقابل، يمكن أن يعزى غياب خدمة الانترنيت في بعض المساكن بإيران (والتي بلغت نسبتها حوالي 51 % من عموم المساكن المتوفرة بإيران في عام 2015) الى جملة من الأسباب، أهمها (*ITO,2015*): عدم إحساس أرباب المساكن بحاجتهم الى خدمة الانترنيت (64 %)، أو غياب الخبرة باستخدام الانترنيت (30%)، أو نتيجة لارتفاع أجور الخدمة (18%)، أو ارتفاع كلف أدوات المعلومات والاتصالات (17%)، او عدم توفر الخدمة في المنطقة الجغرافية (10%)، أو الاكتفاء باستخدام الانترنيت خارج حدود المسكن (6%)، أو لأسباب ثقافية (2 %)، او خشية من أمور تخص المسائل الأمنية (1 %).

وتسافر هذه الخدمة السيبرانية عبر شبكة واسعة من الألياف البصرية تغذي عموم المحافظات الايرانية بخدمات الانترنيت، وشبكات المعلومات المحلية، بلغ طول أليافها حوالي 54,135 كيلومتراً، يتم تغذيتها بواسطة 13,357 محطة ثانوية للأقمار الصناعية، بينما يبلغ حصة المواطن من حزمة خدمة الانترنيت المتوفرة بالبلاد حوالي *8.2 Kbps* وهي سعة متواضعة إذا ما قورنت بدول المنطقة (*19 Kbps* في الدول العربية، *21Kbps* دول الجوار الإيراني) (*ITU,2015*).

2 . 1 . 3 . وفرة الحواسب:

نجحت الآلة التقنية الإيرانية في تصنيع حواسب بأسعار مناسبة، كثر استخدامها في المجتمع الإيراني في ظل الحصار المفروض على البلاد، وتوفرت على التوازي مع الحواسب التي ترد البلاد من مصادر انتاجها في بلدان جنوب شرقي آسيا، وأوربا، والولايات المتحدة.

أظهر المسح الميداني الذي قامت به كوادر مؤسسة تقنية المعلومات الإيرانية، أن الحواسب المنضدية *Desktop* قد احتلت المرتبة الأولى بين المستخدمين الإيرانيين وبنسبة انتشار بلغت 84.1 %، في حين أتت الحواسب المحمولة *Laptop* بالمرتبة الثانية، وبنسبة انتشار بلغت 31 %، بينما جاءت الحواسب اللوحية *Tablets* بالمرتبة الثالثة وبنسبة انتشار بلغت 22 %، بينما لم تتجاوز نسبة الحواسب اليدوية *Handheld* 1.2 % (*M.o.ICT,2015*).

أما حجم إقبال المواطن الإيراني حسب الفئات العمرية، فيمكن مراجعته في الجدول (1 - 5). ويبدو واضحاً أن فئة الشباب (15-24 سنة) يمثلون الشريحة الأكثر استخداماً للحواسب، وبنسبة بلغت 51.2 %، بينما تأتي فئة الراشدين (25-49 سنة) بالمرتبة الثانية، وبنسبة بلغت 33.6 %، ويأتي المسنين بمرتبة تسبق الصغار.

الجدول (1 - 5) ـ إقبال الفئات العمرية للمواطن الإيراني على استخدام الحاسب.

الفئة العمرية	نسبة الاقبال على الاستخدام
14-6 سنة	% 18.7
24-15 سنة	% 51.2
49-25 سنة	% 33.6
74-5 سنة	% 20.2
أكبر من 74 سنة	% 1.8

المصدر: *M.o.ICT,2015*.

2 . 1 . 4 . مجهزي خدمة الانترنيت *ISP's*:

تقوم كل من شركة اتصالات المعلومات الإيرانية *DCI*، (والتي تعمل تحت مظلة شركة الاتصالات الإيرانية *TCI*) وعلى التوازي مع منظمة البحث للعلوم والتقنية الإيرانية *IROST* بمهمة تجهيز خدمة الانترنيت لاالفضاء السيبراني الحكومي بإيران.

اما على صعيد نشاط القطاع الخاص، فهناك الشركة العملاقة *Pars.net* التي تقوم بتوفير الخدمات السيبرانية في طهران، وشركة *Irangate.net* التي تستوطن محافظة أصفهان. وينتشر بعموم الرقعة الجغرافية لإيران، عدد كبير من الشركات المحلية التي تنهض بمهمة تجهيز خدمة الانترنيت للقطاع الخاص والمواطنين، منها: *Shatel, Mobinnet, Sepanta, Pars Online, Sharhad Network, CTEL Kish*، وغيرها من شركات تجهيز الخدمة الى ناهز عددها 1,223 شركة (منها 12 شركة مرخصة بتجهيز خدمة الانترنيت بالسرع العالية) من شركات القطاع الخاص التي لا زالت ترتبط بالقطاع الحكومي الذي يهيمن على حركة المرور السيبراني بالبلاد. وتقوم شركة إيران للاتصالات *TCI* بتحديد سعة تجهيز خدمة الانترنيت لجميع الشركات المجهزة لخدمة الانترنيت في إيران وعلى أساس سعة الحزمة الدولية من جهة، والتوجهات السياسية للدولة تجاه المتغيرات السياسية لكل مرحلة من المراحل التي تمر بها البلاد.

وبالنسبة لسرعة الخدمة، فقد تميزت إيران في بدايت دخولها الى الفضاء السيبراني بسرع انترنيت متباطئة جداً، نتيجة للإجراءات المتعسفة التي اعتمدتها الحكومة لكف الأنشطة التي تعد محظورة وفق خطاطتها السياسية والعقدية. بالمقابل سعت الإدارة السيبرانية بالبلاد الى زيادة سرعة الخدمة بعد توظيف تقنيات المراقبة والترشيح، فبلغت السرعة حوالي *128 KBps* في تسعينيات القرن الماضي، ثم حصلت طفرة أخرى على صعيد سرعة الخدمة بحيث بلغت *2MBps* في عام 2014، والتي لا تكاد تبلغ عشر متوسط سرعة الخدمة المتوفرة في عموم بلدان العالم (*Rezian,2014*).

وتتنافس مع شركة إيران للاتصالات *TCI*، 11 شركة خاصة لتجهيز الخدمة *PAPs* على الحصص المتوفرة في سوق توفير خدمات الانترنيت، وذلك عن طريق طرح الخدمة عبر تقنيات *ADSL2+WiMAX*. بالمقابل تشرف شركة تقنية المعلومات *ITC* (والتي تعد من فروع شركة إيران للاتصالات) تطوير شبكة إيران الوطنية للبيانات المرتكزة الى عنونة *IP*، وتوزع من خلالها خدماتها على حوالي 210 مدينة إيرانية، وبمنافذ خدمة سريعة تصل الى 60 ألف منفذ، وذلك لتلبية احتياجات مختلف القطاعات في البلاد.

2 . 1 . 5 . الجغرافية السياسية للارتباط السيبراني في إيران:

حتم الموقف (المناهض لكل ما يرتبط بالغرب) الذي تتخذه الثورة الإسلامية في إيران، والموقف المتشدد الذي يتبناه المرشد الأعلى الامام علي خامنئي عدم اعتماد مبدأ الاستخدام المفتوح لشبكة الانترنيت، مع استمرار مراجعة النظر في عقد ارتباطاتها السيبرانية بموارد الشبكة العولمية، مع الاعتناء باختيار مساراتها وفق خطاطة جيوسياسية تتوافق مع أولويات الأمن القومي، ومبادئ الثورة الإسلامية التي تحددت ملامحها الجوهرية منذ عام 1979.

في بداية الأمر، وعند بلوغ الخدمة السيبرانية رقعة واسعة من الأراضي الإيرانية، انشغلت المؤسسات الأكاديمية، والوزارات بعناصر الفضاء، والموارد السيبرانية الخصبة التي يمكن أن توفرها للمستخدمين، وللفرص التي يمكن أن تدعم بها بيئة البحث والتطوير، والآلة الصناعية، والمنظومات الدفاعية. بيد أن توسع دائرة استخدام الانترنيت، وتغلغلها في جل تفاصيل الحياة اليومية للمواطنين، وغياب الحدود المكانية للخطاب المطروح فيها، وانفتاحها التام على المنظومة العولمية بات يشكل قلقاً متزايداً لدى الإدارة الحكومية، مع تفاقم من حجم الضغوط وسهام النقد التي باتت توجه من المنظومة العقدية بالبلاد، والحرس الثوري الإيراني الذي بات يستشعر نمواً متزايداً في المخاطر المحتملة، التي يمكن أن تهدد أهداف الثورة، وتؤثر على الكثير من غاياتها وتوجهاتها الحالية والمستقبلية.

فلم تجد وزارة تقنية المعلومات والاتصالات الإيرانية بداً من لملمة جميع تفرعات الشبكة السيبرانية، الأكثر تمدداً، وتعقيداً في منطقة الشرق الأوسط، وإجبار جميع عقدها السيبرانية على الارتباط الصارم ببوابة المنظومة السيبرانية لشركة إيران لتناقل البيانات *DCI* والتي يرتبط ولاؤها بالمؤسسة الحكومية[6]. وقد وفّر هذا الخيار المتشدد للحكومة الإيرانية فرصة الهيمنة المطلقة على حركة المرور السيبراني الإيراني، والتحكم بالمحتوى السيبراني، ومراقبته، وترشيح مادته من أي خطاب قد يتعارض مع خطاب الثورة ومبادئها.

بالمقابل فرضت الخطاطة الاقتصادية الجديدة للقرن الحادي والعشرين، وبما تحتمه من انفتاح على المنظومة العولمية لاقتصاد المعلومات والمعرفة، ضغوطاً معاكسة على الإدارة الحكومية بإيران، ولم يعد ممكناً الانعزال عن الفضاء الاتصالي العولمي، والتفاعل مع مجتمعات المعلومات والمعرفة، عبر فيض رقمي منفتح بالكلية على الآخر.

من أجل هذا تحتّم على الإدارة الحكومية التوجه نحو الموازنة بين ضرورة تطوير المنظومة الاقتصادية والتقنية بالبلاد، من جهة، والحفاظ على سلامة الفضاء السيبراني من عمليات الاختراق المحتملة، وحماية بيضة الثورة الإسلامية في البلاد، من جهة اخرى. فلم تجد وزارة تقنية المعلومات والاتصالات إلا أن تحدد بعناية مسارات للارتباط السيبراني تؤمن استدامة الخدمة في البلاد، مع ضمان مستوى مقبول من التنوّع في موارد الاستخدام، لتوفير فرصة المناورة مع ما قد تفرضه التغيرات على الساحة الجيوسياسية لمنطقة الشرق وما يعصف بها من أحداث متسارعة، على ألا يغيب عن بال الإدارة السيبرانية ضرورة السيطرة المركزية على الفيض السيبراني الذي يتدفق عبر شبكات المعلومات في عموم إيران. كما ن الأمن السيبراني لإيران يحتم وجود أكثر من مورد لتجهيز الخدمة بحيث يمكن تفويت الفرصة على أعداء الثورة بحجب الخدمة عن إيران لأي سبب كان، وجعل زمام قرار إيقاف الخدمة بيد الإدارة الحكومية الإيرانية، متى وجدت موجباً لاتخاذ مثل هذا القرار، دون غيرها.

[6] . يدّعي البعض أن هذا الشركة تدار بإشراف مباشر من قبل الحرس الثوري الإيراني.

لقد قامت وزارة تقنية المعلومات والاتصالات بربط إحدى عقدها السيبرانية ـ الأساسية مع تركيا، وعبر الجزء الشمالي الغربي من البلاد، من تبريز باتجاه العاصمة التركية، أنقرة، ومدينة إسطنبول على التوازي مع خطوط نقل الغاز الطبيعي، وبالتنسيق مع شركة *TTnet* التركية.

أما العقدة الثانية فقد اجتازت أليافها البصرية مياه الخليج العربي باتجاه دولة الامارات العربية المتحدة قبل أن تلج الأراضي الايرانية.

وقد استثمرت إيران الموقف السياسي الروسي الداعم لإيران لمناهضة موقف الغرب، بالشروع في مدّ عقدة ربط معلوماتية جديدة وبالتنسيق مع شركة *RoseTelecom* الروسية لتوفير ارتباط بالفضاء السيبراني لخدمة الانترنيت (*Renesys,2011*).

وعلى هذا الأساس نجحت إيران في استثمار المناخ الجيوسياسي بالمنطقة لتوفير مورد أكثر اماناً تجهيز الخدمة للبلاد، مع القدرة على التعامل مع أية متغيرات جديدة لضمان استبقاء سريان الفيض السيبراني باتجاه إيران.

2 . 2 . مجالات توظيف أدوات المعلومات والاتصالات في المجتمع الإيراني:

حرصت الإدارة الحكومية في إيران على توظيف أدوات المعلومات والاتصالات في الكثير من مفاصل الأنشطة التي تسود المجتمع الإيراني، وسعت الى تخصيص ميزانية ضخمة لدعم عملية التوظيف وتوجيهها باتجاه مسارات تخدم خططها التنموية. وتظهر المراجعة الميدانية لتفاصيل هذه المسألة أن إيران كانت الرائدة بين جلّ دول المنطقة على صعيد توظيف الخطاطة الالكترونية في إدارة الكثير من الأنشطة السائدة في مجتمعها المعاصر، بيد أن دوامة الحرب مع العراق في الثمانينات، والأحداث السياسية المتلاحقة التي عصفت بالبلاد، مع وجود المعارضة المتشددة إزاء إدخال تقنيات قد يشكّل حضورها تهديداً على المستويين العقدي، والأمني، مع الحصار بسبب أزمة الملف النووي قد أسهم بتحجيم النشاط، لحد ما، بيد أن جميع هذه التحديات مجتمعة لم تحول دون بسط كم كبير من مجالات التوظيف السيبراني، داخل حدود المجتمع الإيراني المعاصر.

2 . 2 . 1 . التعليم المدعم بأدوات المعلومات والاتصالات:

لم تكتفي الإدارة الحكومية الإيرانية بالتوسّع الماموثي في أعداد الطلبة الملتحقين بمؤسسات التعليم العالي التقليدي في عموم البلاد، فوجهت المزيد من عنايتها الى توظيف أدوات المعلومات والاتصالات لتوطين أنشطة التعليم التي ترتكز الى أدوات المعلومات والاتصالات ضمن منظومة التعليم العالي ـ الإيرانية (*Yaghoubi, et.,al.,2008*).

فنجحت إدارات التعليم العالي في توطين نمطين من أنماط التعليم المدعم بأدوات المعلومات والاتصالات، (الأول): التعليم عن بعد، والذي سبق حضور أدوات التعليم الالكتروني، بيد أنه قد حسّن أداءه، بشكل ملموس، بعد بلوغها الى الفضاء الاتصالي بالبلاد، و(الثاني) : التعليم الالكتروني الذي يعد نتيجة مباشرة لتوظيف أدوات المعلومات والاتصالات في تسيير عملية التعليم في مجتمعات المعلومات المعاصرة.

2 . 2 . 1 . 1 . التعليم عن بعد Distance Education:

توظف عملية التعليم عن بعد طيفاً واسعاً من تقنيات التعليم، التي اعتمدت، في بداياتها، مبدأ توزيع المناهج عبر خدمات البريد، وبواسطة وسائط منطوقة، أو مرئية. وبعد تغلغل أدوات المعلومات والاتصالات، وخدماتها السيبرانية،

بدأت هذه التقنية بدعم عملية التعليم عن بعد من خلال برامج التدريب المرتكزة الى الحاسب *CBT*، والمادة المودعة في الأقراص الممغنطة والليزرية، ومواقع شبكة الويب العولمية.

وتتميز عملية التعليم عن بعد بكونها تجرى بنسق غير متزامن *Asynchronously* ذلك لأن الطالب يستقر بعيداً عن أستاذه، ويمارس واجباته الدراسية بنسق يتلاءم مع الزمن المتاح له، وبحسب معطيات الرقعة الجغرافية التي يستوطنها، بيد أنه يلتزم بالنظام الداخلي للعملية التعليمية وتوقيتات اختبارات منهج الدراسة الجامعية.

شجعت الإدارة الحكومية الإيرانية عملية التعلّم عن بعد لتلبية سياستها في زيادة عدد الطلبة الإيرانيين الملتحقين بالتعليم العالي، ولتجاوز عقبة تمويل العملية التعليمية متجاوزة ظاهرة شحة موارد البنية التحتية التي تفتقر إليها عملية التعليم، وقلّة الكوادر التدريسية الاحترافية، من جهة، ولمنح طلبة القرى والمدن الإيرانية النائية، فرصة تطوير تحصيلهم الدراسي مع شحة الموارد المالية التي تمتلكها عوائلهم لتلبية متطلبات الالتحاق بالتعليم العالي.

كانت جامعة آزاد المفتوحة، اول مؤسسة جامعية توظف مبدأ التعلم عن بعد في إيران، والتي فتحت أبوابها للالتحاق الطلبة في عام 1975 والتواصل بمادتها التعليمية من خلال نسخ المناهج المطبوعة التي أرسلت للطلبة عبر خدمة البريد المحلي، بينما وفرت دعماً تعليمياً لطلبتها عبر الدروس التي بثّت عبر برامج موجهة لقنوات الراديو والتلفزيون بعموم البلاد (*Masoumi,2010*).

2 . 2 . 1 . 2 . التعليم الالكتروني *e-Learning*:

بعد أن تبنت وزارة العلوم والبحوث والتقنية *MSRT* سياسة لا مركزية بالتعامل مع الجامعات والمعاهد، ومراكز البحث العلمي، توفرت أكثر من فرصة سانحة لهذه المؤسسات لتبني برامج تطويرية مستحدثة على صعيد نظمها التعليمية والتدريبية.

فباشرت بزج تقنيات المعلومات والاتصالات وأدواتها لدعم أنشطتها التعليمية، والتي أسهمت الى حد كبير في تخفيض النفقات، وتوسيع مجال بلوغ خدماتها الى رقعة جغرافية واسعة من إيران. وكان نهج التعليم الالكتروني من الخيارات التي يمكن أن تستثمر القدرات الفريدة التي توفرها أدوات المعلومات والاتصالات السيبرانية في صناعة مناخ مناسب لترويج التعليم العالي ـ الالكتروني، وباستثمارات يمكن توفيرها محلياً، لإنشاء معاهد وجامعات افتراضية *Virtual Institutes & Universities*.

وقد ألحقت الكثير من الجامعات الإيرانية أنظمة التعليم الالكتروني بنظمها التقليدية، فكانت البداية مع الجامعات الحكومية، منها: جامعة شيراز، وجامعة إيران للعلوم والتقنية، وجامعة امير كبير، وجامعة الطوسي، وكلية علوم الحديث، وجامعة أصفهان، وجامعة الشهيد بهشتي، وجامعة طهران. ثم التحقت بها الجامعات والمعاهد الخاصة، منها: معهد طهران للتعليم العالي، ومركز نور للتعليم العالي، وجامعة المصطفى المفتوحة، وجامعة طهران الطبية، والتي عمدت جميعاً الى إنشاء بوابات رقمية لجامعاتها ومعاهدها الافتراضية، ويؤمل ان تلتحق بهذه الجامعات، جامعات أخرى، مثل: جامعة شريف للتقنية، وجامعة تربية المدرس، وجامعة زنجان، ومعهد الفارابي للتعليم العالي (*Masoumi,2010*).

وقد اشترطت وزارة العلوم والبحوث والتقنية على هذه المؤسسات التعليمية ـ الافتراضية، الالتزام بالمناهج والبرامج الأكاديمية التي تعتمدها الوزارة، ونظمها للاعتراف بشهادة الطلبة الملتحقين بها.

ودشّنت جامعة شيراز أول برنامج للتعليم الالكتروني بين الجامعات الإيرانية في بداية عام 2004، وقد تزايدت أعداد المعاهد والمراكز الافتراضية التي هرعت مؤسسات التعليم العالي الحكومي والخاص فبلغ عديدها ثمانية مراكز افتراضية خلال السنوات الأربع التي تلت المشروع الرائد لجامعة شيراز. وبدأت أعداد الطلبة الملتحقين بهذا النمط من التعليم تتزايد تدريجياً (رغم محدوديتها بالمقارنة مع الأعداد الهائلة للطلبة الملتحقين بمؤسسات التعليم العالي ـ التقليدية) ـ أنظر الجدول (1 - 6).

الجدول (1 - 6) ـ توزيع الطلبة الإيرانيين على المعاهد الافتراضية خلال السنوات 2004-2007.

المعهد	العام الدراسي				المجموع
	2004	2005	2006	2007	
معهد شيراز الافتراضي.	115	317	320	507	1259
معهد أوست الافتراضي.	...	297	572	1108	1977
معهد الحديث الافتراضي.	...	180	252	789	1221
معهد أمير كبير الافتراضي.	120	120	120	270	630
معهد الطوسي الافتراضي.	...	200	110	450	760
معهد أصفهان الافتراضي.	...	...	12	114	126
معهد بهشتي الافتراضي.	...	...	...	269	269
معهد طهران الافتراضي.	...	...	...	600	600
معاهد أخرى متفرقة.	...	...	611	811	1422
المجموع	235	1114	1997	4918	8624

المصدر: *Masoumi,2010*.

وشهد عام 2004 التحاق 235 طالباً بمعهدين افتراضيين، ثم تكاثرت أعداد المعهد، شيئاً فشيئاً، مع تزايد أعداد الطلبة المقبلين على الدراسة فيها، بحيث بلغ عدد هذه المعاهد أكثر من عشرة معاهد، بينما بلغ عديد طلبتها 8,624 طالباً.

بصورة عامة، اتسم نظام التعليم الالكتروني وانصبغ بصبغة إيرانية محلية، فلم يأتي بمناهج وطرائق تدريس جديدة، وإنما كان عبارة عن نسخة رقمية لمناهج الجامعات التقليدية، وتحوّل المدرس من قاعة الدرس باتجاه الفضاء السيبراني، ولم تسهم هذه المعاهد، ورغم كثرتها، في تطوير المناهج، أو النهج التعليمي، وإنما اقتصر دورها على تخفيف الأعباء عن مؤسسات التعليم العالي ـ التقليدية التي ازدحمت أروقتها بالطلبة المقبلين بشغف على الدراسة والتحصيل العلمي (*Omidinia,et.,al.,2010*).

2 . 2 . 2 . تطبيقات الصحة الالكترونية *e-Health*:

كانت بداية سنة 1990 نقطة الشروع لتوطين خدمات الصحة الالكترونية، عندما استخدم تطبيق برمجي، أعدته الكوادر الإيرانية، لإدارة عملية تسجيل المرضى والمراجعين للمؤسسات الصحية. ثم بدأت مؤسسة الأمن الاجتماعي بتوظيف تقنيات السيبرانية في مراكزها وفق المعايير المعتمدة دولياً (*MohammadJavadi&Saadi,2010*).

وقد أسهم البرنامج الوطني الإيراني لتقنية المعلومات *TAKFA* الذي تبنته الحكومة الإيرانية في عام 2002 في ولوج النظام الصحي الى الفضاء السيبراني الفسيح، والذي تجلت بواكيره مع ولادة أول نظام وطني لإدارة السجلات الصحية، والذي أطلق عليه اسم *SEPAS*.

ثم أبصرت، بعد مدة قصيرة، المعمارية المقترحة لإدارة أنشطة الرعاية الصحية في إيران، والتي تضمنت ثلاث مستويات لتنفيذ النظام السيبراني ـ الجديد على أرض الواقع (*MohammadJavadi&Saadi,2010*):

المستوى المحيطي: المستوى الأول لنظام المعلومات:

اقتصار عملية ربط قواعد بيانات النظام الصحي السيبراني بالمعدات الطبية، والأجهزة والمعدات السيبرانية المحمولة ضمن حدود المؤسسة ذاتها، وذلك لوجود صعوبات تقنية لتكامل البيانات على المستوى الوطني.

المستوى الوسيط: المستوى الثاني لنظام المعلومات:

وتضمنت تنصيب النظام وتشغيله ضمن مراكز توفير الخدمات الصحية في البلاد.

المستوى المركزي: المستوى الثالث لنظام المعلومات:

وتضمنت تنصيب النظام في وزارة الصحة والجامعات والمعاهد الطبية في عموم البلاد لتوفير البنية التحتية الداعمة لعمل النظام، وضمان تكامل عمله في عموم إيران.

وقد أظهر التقييم الذي قامت به كوادر منظمة الصحة العالمية لنظام الصحة الالكترونية عام 2012 أن وزارة الصحة في إيران قد بذلت جهوداً مكثفة لتوطين تقنيات الصحة الالكترونية بيد أن هذه الجهود لم تؤت ثماراً ناضجة، بسبب عدم تكامل البرنامج والسياسات التي تبنتها هذه الوزارة، وشحة الموارد، وعدم كفاية التخصيصات المالية لدعم البرنامج الجديد، وعوامل أخرى.

وقد حاولنا بيان أهم المحاور التي تضمنتها المراجعة التي قام بها خبراء منظمة الصحة العالمية والتي ستوفر امامنا صورة جلية لواقع نظام الصحة الالكترونية في إيران، والذي لازال يعاني من الكثير من العقبات لغاية هذا التاريخ (*WHO,2012*):

المحور الأول: الإطار العام للسياسة الطبية ـ الوطنية:

تبنت الحكومة الإيرانية خطوات إيجابية تجاه السياسة الوطنية لحكومتها الالكترونية، بيد أن تنفيذ هذه السياسة لا زال جزئياً ولم يشمل الالتزام بجميع تفاصيلها بالإضافة الى غياب موعد محدد لاستكمال هذا المشروع. وفي الوقت ذاته يلاحظ أن هناك لدى وزارة الصحة والجهات ذات العلاقة بالملف الصحي سياسة واضحة لتوطين تقنيات

وخدمات الصحة الالكترونية في إيران، بيد أن السقف الزمني المحدد لتنفيذ البرنامج عام 2007 لا زال مفتوحاً، ولا زالت عملية التنفيذ غير متكاملة على أرض الواقع لغاية هذا التاريخ.

بالمقابل لا تتوفر بيانات شافية بصدد استكمال سياسة أدوات المعلومات والاتصالات ذات الصلة بالقطاع الصحي، وكذلك الحال بالنسبة لسياسة العلاج عن بعد *Telemedicine Policy* والتي لم توليها وزارة الصحة الإيرانية أي اهتمام يذكر، أسوة بغيرها من التطبيقات السيبرانية الصحية.

المحور الثاني: الإطار القانوني والأخلاقي للصحة الالكترونية:

رغم محاولات وزارة الصحة تنفيذ مستلزمات هذا المحور إلا أن ساحته لا زالت مليئة بالفجوات التي نشأت عن عدم وجود استجابة حقيقية لمؤسسات القطاع الصحي في كثير من المحاور. ومما يسترعي الانتباه هو عدم وجود أي تحرك على صعيد تفعيل التشريعات ذات الصلة بقطاع الصيدلانيات السيبرانية، مع غياب أدوات بسط أمن الانترنيت بحيث تكف عمليات شراء الأدوية خارج حدود التشريعات الطبية المعتمدة.

المحور الثالث: نفقات الصحة الالكترونية ومصادر التمويل:

نجحت وزارة الصحة بالحصول على التمويل المطلوب للقطاع الطبي الحكومي فاستطاعت توفير أدوات المعلومات والاتصالات، والبرمجيات، والمشاريع الريادية، ودعم الزمالات الدراسية. بالمقابل يلاحظ غياب اهتمام الحكومة بمضمار تمويل نشاط القطاع الطبي ـ الخاص، مع عدم وجود أي نشاط حاول جلب المتبرعين لدعم النظام السيبراني الجديد. بالمقابل نلاحظ بروز شراكات بين القطاع الحكومي والقطاع الخاص *PPP* على صعيد توفير التطبيقات البرمجية الداعمة لتوطين أنظمة الصحة الالكترونية، ورعاية المشاريع الطبية الريادية.

المحور الرابع: بناء القدرات الوطنية:

أشار المسح الميداني لكوادر منظمة الصحة العالمية الى وجود فراغ شبه تام على صعيد برامج بناء القدرات البشرية لتصميم، وتنفيذ، وتشغيل تطبيقات الصحة الالكترونية في إيران. فلا توجد مقررات تدريبية للطلبة في مؤسسات التعليم العالي ـ الطبية لبناء قدرات الطلبة وتعميق مهاراتهم بالتعامل مع نظم الصحة الالكترونية. كما أن الجهات التي تعنى بتطوير الموارد البشرية الطبية لم توجه اهتمامها نحو برامج التعليم المستمر للكوادر الطبية لمتابعة التطورات الحاصلة في النظام، وكيفية استثمار قدرته في تطوير نظام الرعاية الصحية في مؤسساتهم الطبية.

المحور الخامس: تطبيقات الصحة الالكترونية:

أكد تقرير لجنة منظمة الصحة العالمية على وجود فجوة في مجال التطبيقات البرمجية لنظام الصحة الالكترونية. فلا زال تطبيق العلاج عن بعد يفتقر الى سياسة واضحة، وأرضية تشريعية داعمة، أو معايير وطنية واضحة لهذا النشاط، يضاف اليه غياب المعرفة التقنية بهذا المجال، لذا لا يتوقع تفعيل هذا النشاط بصورة سليمة خلال المستقبل القريب.

اما بالنسبة لبرامج التعليم الالكتروني لطلبة مؤسسات التعليم الطبي العالي فلا زالت التطبيقات محصورة في قطاع تدريب الكوادر الطبية الاحترافية، بينما لا زالت برامج تدريس العلوم الطبية غير ناضجة بالمستوى المطلوب.

2 . 2 . 3 . أنشطة التجارة الالكترونية في إيران:

تشمل التجارة الالكترونية مجموعة الأنشطة التي توظف أدوات المعلومات والاتصالات لتبادل وترويج السلع والخدمات التجارية ـ التقليدية عبر القنوات الاتصالية التي يوفرها الفضاء الاتصالي لشبكة الانترنيت، وشبكات المعلومات المحلية، وتسليع المعلومات (النصوص، والوسائط المتعددة)، والموارد المعرفية (الخبرات التي تستنبط بواسطة آليات المعالجة الذكية) لتحقيق قيمة اقتصادية مضافة (*Rasoolian,2010*).

لقد حدد الإطار العام لسياسة الحكومة الإيرانية لدعم وترويج أنشطة التجارة الالكترونية من خلال ما ورد بالمذكرة التي صودق عليها من قبل هيئة الوزارات في عام 2002، والتي تضمنت ضرورة التزام الحكومة بتوفير ما يأتي لإنجاح هذا القطاع الاقتصادي الحيوي من خلال مجموعة خطوات تضمنت(*Abbas,2007*):

- ✓ ضرورة توفير البنية التحتية الأساسية مع التشريعات الداعمة، لمجالات الأنشطة التي يمكن أن تنمو التجارة الالكترونية في بيئتها مع ضمان استدامتها.
- ✓ لتطوير تطبيقات وطنية للتجارة الإلكترونية وبناء قدرات محلية لاستخدامها بشكل سليم.
- ✓ التحوّل نحو دعم القطاع الخاص للمساهمة في هذا القطاع، والسعي نحو حلحلة الهيمنة الحكومية لتنشيط فرص التنافس بالسوق لضمان توسعه ونموه.
- ✓ السعي نحو إزالة العقبات التي قد تقف أمام هذا النشاط والسعي الى تذليها على المستويين التقني والتنظيمي.
- ✓ توسع دائرة استخدام خدمة الانترنيت لأغراض التجارة الالكترونية، مع إدامة المراقبة على سلامة المحتوى المطروح في فضاء التجارة السيبراني.

وقد هرعت الوزارات والمؤسسات المعنية بهذا الأمر، وكل حسب اختصاصها، الى الالتزام بما ورد في هذه المذكرة، مع السعي الى ترجمة مضامينها الى إجراءات يمكن تنفيذها على أرض الواقع لتوفير مناخ مناسب لولادة سليمة لأنشطة التجارة الالكترونية في البلاد ـ أنظر الجدول (1 - 7).

الجدول (1 - 7) ـ توزيع المهام والمسؤوليات على المؤسسات والوزارات الإيرانية بموجب مذكرة دعم التجارة الالكترونية لعام 2002.

المؤسسة أو الوزارة	المهمة المحددة	الجهات الداعمة
وزارة تقنية المعلومات والاتصالات *MCIT*	توفير عتاد الحواس وملحقاتها، والبرمجيات التي يتطلبها النشاط، مع توفير بيئة اتصالية آمنة، وبسرعة انترنيت عالية، مع السعي الى تقليل كلف الاستخدام الى الحد الأدنى.	....
وزارة الشؤون الاقتصادية والتمويل	لتوفير تفاصيل التحويل المالي السيبراني للمشروع مع تشغيل خدمات بطاقات الائتمان.	المصرف المركزي ومصارف أخرى

المؤسسة أو الوزارة	المهمة المحددة	الجهات الداعمة
وزارة التجارة MC	دارسة الجدوى الفنية والاقتصادية ـ التفصيلية لمشروع التجارة الالكترونية مشفوعاً ببرنامج التنمية ـ طويل المدى للتجارة الالكترونية.	...
	لتنفيذ المرحلة الريادية Pilot Project لمشروع التجارة الالكترونية لتوفير أرضية آمة للصفقات الالكترونية ـ الداخلية والخارجية، وتوفير الخدمات اللازمة لدعم تنفيذ مشاريع مشابهة في القطاع الخاص.	
	إجراء برامج تدريبية ـ احترافية، قصيرة المدى، وعقد ندوات محلية وأخرى وطنية لتعميق المعرفة بالتجارة الالكترونية وممارساتها.	
	جذب وتشجيع الاستثمار الوطني والأجنبي وفق الإطار العام للتشريعات الوطنية الخاصة بالتجارة الالكترونية.	
سكرتارية الهيئة العليا للمعلوماتية *HCIS*	إعداد نظام وطني لسلطات الترخيص على أن يصادق عليها من قبل هيئة الوزارات. إعداد وتوفير مشروع متكامل لصفقات الكترونية ـ آمنة لمراقبة سلامة محتوى المستخدمين في الشبكة العامة بالبلاد.	MC/MCIT/ MSRT/MPO
وزارة العلوم والبحوث والتقنية MSRT	اعتماد مادة التجارة الالكترونية في الجامعات الإيرانية مع عرض فصول دراسية تناقش الأمور التقنية والاقتصادية لهذا الموضوع.	MC/MCIT/HCIS
مؤسسة الإذاعة والتلفاز	لتوفير وبثّ برامج تدريبية حول التجارة الالكترونية.	MC/HCIS
وزارة التجارة *MC*	للتنسيق على صعيد تشجيع ودعم الأنشطة ذات الصلة بالتجارة الالكترونية بين إيران وجهات مثل: منظمة المؤتمر الإسلامي، مجموعة 77، ECO، خطة Colombo، والهيئات الدولية للأمم المتحدة.	...
سكرتارية الهيئة العليا للمناطق الحرة	لإنشاء مشاريع تجارة الكترونية في المناطق الحرة.	الجهات التنفيذية في المناطق الحرة
مؤسسة الإدارة والتخطيط MPO	لتخصيص تمويل للتجارة الالكترونية ونشر مشاريع الشبكة من خلال الميزانية الوطنية.	الجهة التنفيذية ذات الصلة

المصدر: *Abbas,2007*.

وفي ظل الظروف الحالية، تواجه أنشطة التجارة الالكترونية، في إيران، مجموعة متنوعة من العقبات، فعلى الصعيد اللوجستي، هناك عدم القدرة على الوصول الى برمجيات تجارة إلكترونية مرخصة من الجهات الدولية المنتجة، كذلك صعوبة الوصول الى موارد تحويل النقد الالكتروني (مثل: *PayPal*)، يصاحبه غياب شبه تام للاستثمار الأجنبي في القطاع، وأن الإعلان على مواقع مثل *Facebook*، أو *Google* يعد أمراً مستحيلاً. اما على الصعيد الثقافي والاجتماعي، فهناك المؤسسة الدينية مدعومة بالحرس الثوري الإيراني، والتي تنظر بعين الريبة والشك الى هذا النمط من الأنشطة وتحاول عرقلته بسبب هواجس عقدية وأخرى أمنية صرفه. يضاف الى ذلك ثقافة التجارة التقليدية والتي تفرض ممارسات محددة لعملية البيع والشراء، وعقبات أخرى يصعب حصرها (*Bozorgmher,2014*).

بيد أن هذه العقبات مجتمعة لم تفت في عضد العاملين في هذا القطاع، والذين استطاعوا ترسيخ أكثر من تجربة نجاح على صعيد التجارة الالكترونية في الفضاء السيبراني الإيراني.

حيث تعدّ شركة *DigiKala* أكبر منصة رقمية للتجارة الالكترونية في إيران، توفر من خلال خدماتها الالكترونية مجموعة متنوعة من السلع والخدمات للمواطن الإيراني، حيث بلغت قيمتها السوقية حوالي 150 مليون دولار (*Piran,2014*). وقد حققت هذه الشركة تفوقها في سوق التجارة الالكترونية بالبلاد، بفضل تنويع أنشطتها وعدم قصر نشاطها على بيع وتسويق السلع والخدمات، وإنما توجهت نحو توفير المشورة بخصوص السلع والخدمات للمستهلكين، معتمدة على لفيف من الخبراء والاستشاريين مما رسّخ ثقة المستهلك الإيراني بالسلع المعروضة لديها.

وتهيمن هذه الشركة على حوالي 85 % من صفقات التجارة الالكترونية في إيران، بينما تأتي بعدها شركة *Takhfifan* التي تخصصت بموقعها المخصص للصفقات اليومية، وشركة *Sheypoor*، التي تميزت بعرض إعلانات متخصصة مجانية، وشركة *Zarinpal* وهي شركة تحاكي في نشاطها ،الى حد كبير، شركة *Paypal* (*Dudley,2015*).

وهناك شركة أجنبية وحيدة قد استثمرت في قطاع التجارة الالكترونية بإيران، هي شركة الشرق الأوسط القابضة للانترنيت *MEIH*، وهي عبارة عن مشروع مشترك بين شركة *Germany's Rocket Internet* الألمانية، وشركة اتصالات جنوب أفريقيا *MTN* والتي تعمل في سوق التجارة الالكترونية باسم *Romak* في طهران. وقد أنشأت موقع للتسوّق الالكتروني أطلقت عليه اسم *Bamilo* وموقع *Mozando* لمركز تسوق الكتروني، وموقع *Bodofood* لتقديم وجبات طعام (*Bozorgmher,2014*).

بلغ عدد الشركات الوليدة بمضمار أنشطة التجارة الالكترونية في إيران حوالي 20,000 شركة، لم تنجح حوالي 4,000 شركة منها بالتسجيل لدى المؤسسة الحكومية فبقي عملها خارج الحدود الشرعية (*Piran,2014*).

بالمقابل يوجد حوالي 15,000 موقع إيراني للتسوق الالكتروني بالوقت الراهن (*Dudley,2015*). وتتمتع هذه المواقع بإقبال كبير من المواطنين الإيرانيين بحيث أكدت شركة *MVF* (المتخصصة بكسب العملاء) أن رواد مواقع التسوق الالكتروني في إيران يشكلون حوالي 43% من مستخدمي الانترنيت بالبلاد.

ولا تزال أنشطة التجارة الالكترونية في إيران في بداياتها، ولا تشكّل قيمتها الاقتصادية المضافة (بالوقت الحاضر) سوى 0.7% من الناتج الإجمالي المحلي في البلاد (*Dudley,2015*)، إلا أن بشائر آثار الاتفاق النووي الإيراني مع الغرب، ووجود تسهيلات ودعم للقطاع من قبل حكومة حسن روحاني التي تحاول التخفيف من العقبات التي تعترض هذا

النشاط الاقتصادي المهم، ستسهم الى حد كبير في توسيع الدور الذي يحققه هذا النشاط في منظومة الاقتصاد بإيران، ويتوقع أن يحقق قيمة اقتصادية مضافة الى الناتج الإجمالي المحلي خلال مدة قصيرة، إذا أخذنا بعين الاعتبار:

- ✓ تزايد أعداد الإيرانيين الذين يبحرون في عباب الفضاء السيبراني وبنسب مضاعفة خلال السنتين الأخيرتين نتيجة لتزايد سرعة خدمة الانخفاض، وتراجع كلف الاستخدام.
- ✓ أن نسبة الشباب (الذين تقل أعمارهم عن 35 عاماً) يشكلون نسبة 70 % وهم يقبلون بشغف على استخدام الانترنيت، مع ميلهم نحو التسوق الالكتروني بدلاً من الأساليب التقليدية لتوفيره فرصة خيارات متعددة تتوافق مع رغبة الشباب وطموحهم.
- ✓ تميز المواطن الإيراني بالإقبال الشديد على التسوّق ويمتلك نزعة استهلاكية متميزة رغم الظروف الاقتصادية التي فرضها الحصار على البلاد.
- ✓ وجود توجّه لتوفير دعم على مستوى البنية التحتية للمعلومات والاتصالات، مع تشريعات داعمة لنشر وتوسيع دائرة الفضاء الاتصالي للانترنيت، مع التخفيف من القيود التي كانت مفروضة بالسابق.

وقد افتتح عام 2010 اول مركز تسوق عبر الانترنيت في إيران، هو مركز *Rouyesh Technical Center* ثم افتتح في بداية عام 2011 المهرجان الإيراني الأول للتسوق عبر الانترنيت وبرعاية مباشرة من وزارة التجارة الإيرانية، حيث منحت أفضل شركات التجارة الالكترونية شهادات تقديرية (*Wikipedia,2015*).

وبدأ دور التجارة الالكترونية في المشهد الاقتصادي للبلاد، ينمو بالتدريج حتى بلغ حجم العوائد المتحققة عن أنشطتها المختلفة لعام 2009 حوالي 10 مليارات ريال (أي ما يعادل مليار دولار)، بينما بلغت المبيعات عبر وسائل التسوّق الالكتروني حوالي 300 ألف دولار يومياً في عام 2014، مع وجود أكثر من 20 ألف مخزن مرتبطة بشبكات المعلومات، وتسوّق منتجات إلكترونية متنوعة (*Rezian,2014*).

وقد توقعت مؤسسة بحوث *BMI* حدوث طفرة كبيرة في سوق التجارة الالكترونية بإيران خلال السنوات 2015-2019 كنتيجة حتمية لحسم مسألة الملف النووي الإيراني، إذ سيتوفر مناخ اقتصادي مناسب مع وجود خبرة متراكمة لدى العاملين في هذا المجال بالسوق الإيرانية، رغم محدودية حجم النشاط بسبب ظروف الحصار على البلاد خلال حوالي عقد من الزمان، يضاف الى ذلك الى أن شبكة الاتصالات الإيرانية *MTN* قد أطلقت في النصف الثاني من عام 2014 خدمات جيل الثالث *3G* والجيل الرابع *4G*، حيث ستمهد خدماتها الاتصالية السريعة بيئة داعمة لنمو أنشطة التجارة الالكترونية، على التوازي مع الانفتاح المرتقب (*BMI,2015*).

بيد أن هذا الانفتاح لن يخلو من مخاطر محتملة نتيجة لنظام المراقبة السيبرانية الذي تتبناه وزارة تقنية المعلومات والاتصالات، والضغوط المستمرة للمؤسسة الدينية على الأنشطة التي تعدها تشكل معارضة لمبادئ الشريعة الإسلامية. كذلك لا زالت مؤشرات المخاطر التي وضعتها مؤسسة *BMI* حول فرص انتعاش التجارة في بلد من البلدان غير مشجعة على صعيد: مؤشر المخاطر التشغيلية *ORI*، ومؤشر مخاطر التجارة والاستثمار *TIRI*، ومؤشرات المخاطر اللوجستية، حيث يلاحظ تقدم إيران على العراق، بيد انها لا زالت متراجعة قبالة مصر(*BMI,2015*).

2 . 2 . 4 . تطبيقات المصارف الالكترونية:

تميزت المصارف الإيرانية بسعيها الدائم الى توظيف التقنيات السيبرانية في أنشطتها وخدماتها المصرفية التي توفرها لطيف واسع من زبائنها. وقد أدخلت الى منظومة عملها التطبيقات البرمجية المصرفية، مع إنشاء مواقع لفروعها على الانترنيت، ومنح بطاقات الائتمان لزبائنها، مع توفير أجهزة *Automated Teller Machines ATM*، وأجهزة نقاط البيع *Point of Sell Machines POS*، إضافة الى استثمار شبكة الهواتف المحمولة لتشغيل أنظمة الرسائل القصيرة *SMS* لإخبار زبائنها بحركة الرصيد والانفاق الآني من بطاقات الائتمان. وقد جمعت هذه الخدمات في منصة رقمية موحدة ربطت مع نظام نشرة مجلس الإدارة *BBS* لتوفير جميع تفاصيل الحساب المصرفي، من خلال خدمة هاتفية آلية، وتلقي الفواتير بصورة مباشرة عبر الهاتف المحمول.

ويعد مصرف سامان *Saman Bank* من أوائل المصارف الإيرانية التي طرحت الخدمات الالكترونية المصرفية بالبلاد، وتعوّد الكثير من المواطنين الإيرانيين على استخدام آلات *ATM* لتسديد أجور قوائم: الكهرباء، والهاتف، والهواتف المحمولة، وخدمات الماء والغاز الذي يجهز للوحدات السكنية في إيران (*Davarinejad&Saffari,2011*).

وفي الوقت ذاته، أنشئت شبكة معلومات مصرف *Iran Interbank* للمعاملات المصرفية (وأطلق عليها اسم *Shetab*)، في عام 2002، وأضحت العمود الفقاري لمنظومة المصارف الإيرانية، وأوكلت لها مهمة إدارة وتنظيم الصفقات التجارية من نوع *ATM* و*POS* التي تعتمد على نظام البطاقة الالكترونية. كما انها قامت بالوقت ذاته في الانفتاح على المصارف الخارجية فربطت مصارفها الوطنية مع مصارف في دول مثل: الصين، والامارات، والبحرين، وقطر (*Abbas,2007*).

إضافة الى ذلك تبنت المصارف الايرانية نظم رقمية متقدمة، واعتمدت معايير أمن الأسهم *Security Stock Layer SSL* في أنشطة مصارفها الالكترونية، وروّجت لخدمات المحفظة المالية ـ السيبرانية *e-Purse Service* في الكثير من فروعها المنتشرة بالبلاد.

بدأت شبكة إيران لنقل المعلومات بين المصارف بطرح خدماتها في عام 2002، وذلك لتوفير عمود فقاري متماسك *Backbone* لدعم أنظمة المصارف الإيرانية ـ السيبرانية بحيث تكون قادرة على التعامل مع التعاملات المالية لبطاقة *ATM*، و*POS* وغيرها، الأمر الذي مهد لارتباط تعاملات المصارف الإيرانية مع بقية مصارف البلدان التي لديها علاقات تجارية وثيقة معها مثل: الصين، والبحرين، والامارات، وقطر (*Abbasi, et.,al.,2008*).

وقد أسهم الحصار في فرض قيود كثيرة على أنشطة المصارف الالكترونية، نتيجة لإغلاق الكثير من بوابات التعامل مع المنظومة الاقتصادية العولمية، فلا زالت الخدمات المصرفية الالكترونية متراجعة حيث يلاحظ غياب بوابات الدفع الالكتروني عن المصارف الإيرانية، كما لا زالت المصارف الإيرانية غير قادرة على منح المواطنين بطاقات ائتمان دولية (*Abbas,2007*).

من جهة أخرى، انتعش قطاع المصارف الالكترونية في إيران بحلول عام 2007 نتيجة لالتحاق جميع المصارف الحكومية والخاصة بشبكة النظام الجامع للمصارف الوطنية *Shetab* والتي يديرها المصرف الإيراني المركزي، بصورة غير مباشرة، مع الاستعدادات الجارية لاستكمال مستلزمات تشغيل نظام التسوية الاجمالية بين المصارف الايرانية *RTGS*.

وقد نجحت شبكة *Shetab* في إدارة أكثر من 47.7 مليون عملية مالية شهرياً منذ عام 2007، والتي عدت طفرة نوعية على صعيد إذكاء ظاهرة إقبال الزبائن على المصارف الالكترونية نتيجة لسرعة إنجاز التعاملات المالية وكفاءة أدائها (*Davarinejad&Saffari,2011*). كذلك أعلنت شركة *Tetra-Tech IT* في عام 2007 عن بدء استخدام بطاقات الائتمان من فئة *VISA + MasterCard* في منافذ البطاقات الالكترونية بإيران، وفي مراكز التسوّق، والفنادق، والمطاعم، وشركات السفر للمواطنين الإيرانيين والسواح الأجانب.

وقد أسهم الحصار في فرض قيود كثيرة على أنشطة المصارف الالكترونية، نتيجة لإغلاق الكثير من بوابات التعامل مع المنظومة الاقتصادية العولمية، فلا زالت الخدمات المصرفية الالكترونية متراجعة حيث يلاحظ غياب بوابات الدفع الالكتروني عن المصارف الإيرانية، كما لا زالت المصارف الإيرانية غير قادرة على منح المواطنين بطاقات ائتمان دولية (*Abbas,2007*).

2 . 3 . واقع وبرامج بناء القدرات البشرية اللازمة لإدارة مجتمع المعلومات:

إن الالتزام بعملية الالتحاق بمجتمع معلومات راسخ فرض على الإدارة الحكومية ـ الإيرانية تبني مجموعة من البرامج التي تمنح المواطن القدرة على الانتماء اليه، والمشاركة بالأنشطة، والمهام التي تتطلبها عملية الاستيطان في كيانه المجتمعاتي.

من أجل هذا ينبغي أن تلتزم الإدارة الحكومية بمجموعة من الإجراءات التي توجه اهتمامها نحو بناء القدرات لدى المواطنين على استخدام أدوات المعلومات والاتصالات بشكل سليم لضمان القدرة على الدخول الى الفضاء الاتصالي للمجتمع الجديد، والوصول الى بوابات التعاملات السيبرانية، وبلوغ الموارد المعرفية والخدمات التي يفتقر إليها في حياته اليومية. ولهذا ينبغي أن تتوفر لدى كل مواطن إيراني فرصة الحصول على المعرفة والمهارات التي تعينه على استيعاب طبيعة احتياجاته للحضور الفاعل في البيئة الجديدة، واستثمار الخدمات المتاحة فيها.

ولن يمكن أن تبنى القدرات والمهارات دون وجود نظام تعليمي يعنى بزج مفردات الثقافة السيبرانية، مع وفرة برامج تدريبية للارتقاء بالمهارات والقدرات السيبرانية داخل حدود النظام التعليمي وخارجه. وستسهم هذه البرامج في تعميق ثقة المواطن بالدور الذي يمكن أن تمارسه أدوات المعلومات والاتصالات وترسيخ أمن تعاملاته اليومية، وتوسيع مجالات التطبيقات السيبرانية على جل مساحة الحياة اليومية (*UN,2003*).

وسنحاول خلال تشعبات هذه الفقرة، تتبع سياسة النظام التعليمي في إيران، والمؤسسات التقنية المعنية بتقنية المعلومات والاتصالات لبناء قدرات المواطن الإيراني السيبرانية والاتصالية، وتوثيق صلته بالبوابات والتطبيقات السيبرانية التي تستوطن في تربة المجتمع الجديد.

2 . 3 . 1 . نظام التعليم ودوره في تشكيل ملامح مجتمع المعلومات الإيراني:

تعد عملية التعليم مؤشراً أكيداً على حصاد آفة الأمية، ونمو القدرة لدى المواطن على القراءة والكتابة، وممارسة أنشطة التواصل التي تنتشر بكثافة في مجتمع المعلومات المعاصر. كما أن تطور النظام التربوي، وزيادة الاقبال على المؤسسات الجامعية يعد مؤشراً على بناء القدرات الوطنية، وتوسع قاعدة أفراد المجتمع الذين يمتلكون الوسع على المشاركة في أنشطة مجتمع المعلومات والمعرفة.

ورغم قناعتنا بعدم تطابق خطاطة نظم التعليم السائدة في إيران، وبقية دول المنطقة، مع خطاطة مجتمع المعلومات والمعرفة المعاصر، إلا أن اعتماد مؤشرات عملية التعليم لا زالت ضرورية في تقييم الأرضية الداعمة لبناء القدرات الوطنية على صعيد المساهمة في أنشطة مجتمعات المعلومات حتى لدى المؤسسات، والمنظمات العالمية التي تعنى بتقييم مستويات نضج مجتمعات المعلومات في مختلف البلدان.

من اجل هذا سنحاول مراجعة ملف النظام التعليمي في إيران، سواء على صعيد التعليم الأساسي، أو التعليم العالي، مع تفحص قدرة المواطن الإيراني على ممارسة القراءة والكتابة لأن هذه السمات تعد مؤشرات يمكن أن توفر مناخاً مناسباً، وأرضية متينة لتكامل مشهد مجتمع المعلومات، وبدايات تطوره باتجاه ولادة مجتمع المعرفة.

2 . 3 . 1 . 1 . الإطار العام لنظام التعليم بإيران:

يتألف النظام التعليمي في إيران من خمس مستويات تعليمية: رياض الأطفال، والمدارس الابتدائية، والمدارس الثانوية ـ الدنيا، والمدارس الثانوية ـ العليا، والتعليم العالي. وتشرف وزارتان على هذا النظام التعليمي، وزارة التعليم *Ministry of Education* والتي تنهض بمهمة التعليم الأولي والثانوي، وبرامج تدريب وتطوير الكوادر التربوية، ومدارس التعليم المهني؛ بينما تنهض بمهمة التعليم العالي (على مستوى المعاهد والجامعات) وزارة العلوم والبحوث والتقنية *Ministry of Science Research & Technology* (*NUFFIC,2015*).

بلغ عدد الجامعات الإيرانية 103 جامعة توزعت بين قطاع التعليم العالي الحكومي الذي توفرت لديه: 52 جامعة عامة، و28 جامعة طبية؛ والتعليم الأهلي الذي بلغ عدد جامعاته 25 جامعة. وتعتمد مؤسسات التعليم كافة مبدأ التعليم باللغة الفارسية، مع وجود بعض مؤسسات التعليم العالي التي تدرّس منهجاً محدودة باللغة الإنجليزية.

ويقوم المجلس الأعلى للتخطيط، الذي يتألف من خمسة عشر أستاذاً وعضوية وزير الثقافة والتعليم العالي، بمراجعة جودة التعليم العالي، وإقرار البرامج والمشاريع التربوية التي تعنى بتطوير وتنمية النظام التعليمي في عموم المؤسسة التعليمية الإيرانية. بينما تقع على عاتق وزارة التعليم مهمة متابعة جودة التعليم في مراحل التدريس الابتدائي والثانوي.

2 . 3 . 1 . 2 . التعليم الأساسي:

تبذل وزارة التعليم بإيران جهوداً جبارة للالتحاق بمعايير منظمة *EFA* واللحاق بمعايير منظمة اليونيسيف للارتقاء بمستوى النظام التعليمي لمراحل التعليم الأساسي، والمرحلة السابقة له، مع توسيع قاعدة الفئة القادرة على ممارسة القراءة والكتابة في عموم البلاد.

وقد بلغ عدد الطلبة الملتحقين بمدارس مراحل التعليم الأساسي في بداية عام 2013 حوالي 14,983,300 تلميذاً بلغ عدد طلبة المرحلة الابتدائية منهم 5,974,000 تلميذاً[7].

[7] . حصلنا على هذه المعلومات من الموقع:
http://wenr.wes.org/2013/04/wenr-april-2013-an-overview-of-education-in-iran/

وقد حققت إدارات النظام التعليمي نتائج جيدة، على صعيد تطوير مؤشرات التعليم الأساسي، خلال السنوات 2000-2014 ـ أنظر الجدول (1 - 8).

الجدول (1 - 8) ـ الأهداف التربوية التي حققتها وزارة التربية في إيران على صعيد التعليم الأساسي خلال الأعوام 2003-2014.

المرحلة	الهدف	نسبة ما تم تحقيقه	
		2003	2014
التعليم السابق للتعليم الابتدائي	التحاق الأطفال دون 5 سنوات.	46 %	90 %
	التحاق الأطفال بعمر 5 سنوات.	23.7 %	60 %
	التحاق الأطفال بالمناطق الريفية.	24.4 %	85 %
	مدرسين من حملة الشهادات الجامعية.	45 %	95 %
التعليم الابتدائي والمتوسط	التحاق الطلبة بالدراسة.	108.7 %	102.1 %
	مدرسين من حملة الشهادات الجامعية.	7 %.51	41.8 %
	الانتقال الى المدارس الثانوية.	91.8 %	95.7 %
التعليم الثانوي	التحاق الطلبة بالمرحلة ـ في المدن.	68.7 %	71.4 %
	التحاق الطلبة بالمرحلة ـ في الريف.	...	30 %
القدرة على القراءة والكتابة	الشباب من الجنسين.	82.6 %	81.8 %
	الفئة العمرية (15-24 سنة) ـ الحضر.	94.2 %	96.9 %
	الفئة العمرية (15-24 سنة) ـ الريف.	89.5 %	94.8 %

المصدر: *M.O.E, 2015*.

ويبدو واضحاً أن هناك نمواً ملموساً قد تحقق خلال عقد من الزمان، تطورت خلاله مستويات التحاق الطلبة بالمراحل المختلفة، مع زيادة أعداد الكوادر التدريسية من حملة الشهادات الجامعية، رغم بقاء فجوة بالتعليم الثانوي في الريف الإيراني نتيجة لتراجع نسبة الطلبة المنتقلين اليه من مرحلة التعليم الابتدائي، بسبب الظروف الاقتصادية الصعبة، وميل الأسر الى مشاركة أبنائهم في العمل الزراعي لتلبية الاحتياجات الأسرية.

في الوقت ذاته تناقصت أعداد الفئة الأمية لدى الشباب (فئة 15-24 سنة) فبلغت نسباً جيدة، رغم تراجع نسبة القادرين على القراءة والكتابة لدى الفئة التي يزيد عمرها على 24 سنة، ولكن بنسبة ضئيلة.

كذلك يبدو واضحاً من الجدول (1 - 9) تقارب الجنسين في القدرة على القراءة والكتابة لغاية عام 2011، في حين توازنت الكفة بين الفئتين 1:1 منذ عام 2012، وبنسب تتفوق بها على بقية بلدان المنطقة. الأمر الذي يؤكد قدرة الفئة العمرية الأساسية من الشباب الإيراني على التواصل مع الآخر، والتعبير عن الذات ضمن قنوات التواصل الاجتماعي وغيرها من قنوات الاتصال السيبراني، والتفاعل مع الخدمات التي توفرها الحكومة الالكترونية بإيران.

الجدول (1 - 9) ـ نسبة الشباب الإيراني الذين يحسنون القراءة والكتابة خلال السنوات 2000-2015.

السنة	شريحة الشباب الإيراني (15-24 سنة)			
	نسبة الذكور	نسبة الاناث	النسبة الكلية	مؤشر تكافؤ الجنسين
2000	96.23 %	92.43 %	94.33 %	0.96
2006	97.15 %	96.14 %	96.65 %	0.99
2011	96.6 %	96.07%	96.34 %	0.99
2012	96.89 %	96.72 %	96.81 %	1
2013	96.91 %	96.98 %	96.94 %	1
2014	96.85 %	96.95	96.90 %	1
2015	96.78 %	96.94 %	96.86 %	1

المصدر: *M.O.E,2015*.

2 . 3 . 1 . 3 . التعليم العالي:

بصورة عامة، يختلف التعليم العالي عن التعليم الابتدائي والثانوي، ليس فقط على صعيد الفئة العمرية للملتحقين بمؤسسته التعليمية، ولكن على مستوى توليد وتنمية المفردات المعرفية الجديدة التي تمتد حصيلتها المعرفية في حقول العلم، والثقافة، والاقتصاد، والاجتماع. بيد أن غياب أنشطة وأدبيات البحث العلمي السليم، وفي ظل غياب البيئة الداعمة للابتكار سيسهم في تراجع التعليم العالي *Higher Education* نحو مرتبة التعليم ما بعد الثانوي *Tertiary Education* والتي تلتحق بأنشطة التعليم الذي يسبق مرحلة التعليم العالي.

منذ السنوات الأولى للثورة الإسلامية في إيران، وجه آية الله هاشمي رفسنجاني عام 1982 الى توسيع أرضية التعليم العالي في إيران. وقد ترجم هذا التوجيه من خلال انشاء جامعة آزاد الإسلامية ضمت أكثر من 400 اختصاص علمي وإنساني، وأضحت بعد حين ضمن أكبر ثلاث جامعات بالعالم على صعيد الطلبة الملتحقين بها والذين ناهز عددهم 3.5 مليون طالب في فروعها المنتشرة بعموم الرقعة الجغرافية لإيران.

وفي عام 1988 أنشئت جامعة بايمي نور التي تبنت نهج التعليم عن بعد *Distant Learning* مع منح فرصة الدراسة بأسلوب التفرغ الجزئي، والذي فتح الباب على مصراعيه امام موظفي القطاع الحكومي والخاص للالتحاق بالدراسات الأولية والعليا المفتوحة في أروقتها الأكاديمية. وقد تبنت هذه الجامعة وغيرها من الجامعات الخاصة مبدأ استبعاد اختبار الطلبة للالتحاق بمختلف فروع كلياتها العلمية والإنسانية، الأمر الذي وسّع من قاعدة التعليم العالي بالبلاد من جهة، وأسهم بالوقت ذاته على تحويل الخريجين نحو الالتحاق بالدراسات العليا (الماجستير والدكتوراه) بعد أن ضاقت فرص العمل بحملة الشهادة الجامعية الأولية.

وأضحى التعليم العالي مرتعاً علمياً تتألف مؤسسته التعليمية من أروقة:

- ✓ الجامعات : التي تنقسم الى جامعات عامة، وأخرى شاملة، وجامعات متخصصة (العلوم الإنسانية، الطب، والهندسة)، وجامعات هندسية تطبيقية وتقنية، وجامعة بايمي نور (للتعليم عن بعد)، وجامعات طبية، وجامعات خاصة.
- ✓ كليات إعداد المعلمين.
- ✓ معاهد التعليم العالي.
- ✓ معاهد تقنية وتطبيقية.

وقد توجهت الحكومة الإيرانية نحو توسيع قاعدة التعليم العالي بالبلاد لضمان تطوير قدرات الشباب الإيراني، والظفر بميزة تنافسية وهيمنة في المنطقة، فتزايد أعداد الجامعات ومؤسسات التعليم العالي في إيران من 140 مؤسسة عام 1975 لتبلغ 1080 مؤسسة عام 2014 ـ أنظر الجدول (1 - 10).

الجدول (1 - 10) ـ التوسع في أعداد الجامعات الحكومية والخاصة بإيران خلال السنوات 1975-2014.

السنة	عدد المؤسسات الجامعية الحكومية والخاصة		
	الجامعات الحكومية	جامعة آزاد والجامعات الخاصة	المجموع
1975	100	40	140
1980	210	20	231
1985	120	130	250
1990	105	110	215
1991	120	110	230
1995	150	130	280
2000	250	200	450
2005	270	250	520
2008	280	390	670
2014	320	760	1080

المصدر: *Habibi,2014*.

ويلاحظ توسع قاعدة التعليم الخاص الذي لم تتجاوز نسبتها في بداية عام 1975 حوالي 28.5 % من مجموع المؤسسات لتصل نسبتها الى 70.3 % من مجموع المؤسسات عام 2014.

لقد أنشأت الحكومة الإيرانية جامعة بيام نور المفتوحة لتوفير فرصة التعليم الجامعي ـ عن بعد وبالخصوص للمناطق النائية في إيران، والتي لم تتوفر امام شبابها فرصة الالتحاق بمؤسسات التعليم الجامعي التي تستوطن العاصمة، والمدن الكبرى (*Habibi,2014*). وتتلقى جامعة آزاد دعماً حكومياً كبيراً بالمقارنة مع الدعم المحدود الذي تتلقاه جامعة بيام نور.

بيد أن هذه المعادلة قد انقلبت في عصر الرئيس نجاد الذي وسّع الدعم المالي لجامعة نور على حساب جامعة آزاد كجزء من سياسته المعارضة لسياسة سابقه هاشمي رفسنجاني.

في الوقت ذاته حاول الرئيس نجاد أن يوسّع من حجم الاستثمار في قطاع التعليم العالي ـ الخاص، بعد أن أقر حزمة من التشريعات الداعمة للمستثمرين الذين يرومون إنشاء جامعة خاصة ـ مستقلة. وقد انعكست هذه التسهيلات والدعم الحكومي بجلاء على أعداد الجامعات الخاصة التي ازداد عددها من 50 جامعة في عام 2005 الى 354 جامعة في الربع الأول من عام 2014 (*Habibi,2014*).

وقد أثمر التوجّه الحكومي (نحو زيادة عديد مؤسسات التعليم العالي في إيران)، بشكل جلي، على أعداد الطلبة الإيرانيون، الذين التحقوا بها، أو انهوا دراساتهم الجامعية في أروقتها، بحيث نافس متوسط النمو في أعداد طلبة التعليم العالي النسب التي تحققت في دول المنطقة، بحيث ازدادت نسبة السكان (من الفئة العمرية 25 عاماً وما بعدها) من 0.77 % في عام 1970 الى 18.0 % في عام 2011، بحيث لم تتفوق عليها سوى إسرائيل التي قد حققت تفوقاً متميزاً على صعيد المتوسط العولمي للتعليم العالي.

وكنتيجة مباشرة للتوجه نحو تعزيز مؤسسات التعليم العالي بإيران، ووفرة المقاعد الدراسية التي وفرتها الحكومة الإسلامية لشبابها، تزايدت أعداد الطلبة الملتحقين بمؤسسات التعليم العالي، من 540,000 طالب عام 1991 ليبلغ عددهم 4,367,000 طالب عام 2013 ـ أنظر الجدول (1 - 11).

الجدول (1 - 11) ـ أعداد الطلبة الملتحقين في التعليم العالي بإيران خلال السنوات 1991-2013.

السنة	أعداد الطلبة الملتحقين		
	الجامعات الحكومية	جامعة آزاد والجامعات الخاصة	المجموع
1991	300,000	240,000	540,000
1996	510,000	525,000	1,035,000
2001	700,000	800,000	1,500,000
2005	995,000	1,150,000	2,145,000
2008	1,900,000	1,450,000	3,350,000
2013	2,417,000	1,950,000	4,367,000

المصدر: *Habibi,2014*.

وقد بلغ التعليم العالي في إيران مرحلة متقدمة بين دول المنطقة، واستقرت مؤسساته على قاعدة رصينة من الجامعات، والكليات، والمعاهد، التحق بها عدد كبير من الطلبة الذين لم تقتصر فئاتهم على فئة الشباب، وإنما هرع الكبار من الموظفين العاملين بالقطاع الخاص للالتحاق بمنافذ التعليم العالي المتنوعة للارتقاء بمهاراتهم وخبراتهم، ولضمان تحسين أوضاعهم الاقتصادية والاجتماعية ـ أنظر الجدول (1 - 12).

الجدول (1 - 12) ـ بعض مؤشرات مؤسسات التعليم العالي في إيران لعام 2014.

المؤشر	التفاصيل
عدد الجامعات ومؤسسات ومعاهد التعليم العالي.	500
عدد الجامعات ومؤسسات ومعاهد التعليم العالي ـ غير الحكومية.	2,000
عدد الكوادر التدريسية في الجامعات والمؤسسات والمعاهد الحكومية.	59,886
عدد الكوادر التدريسية في الجامعات والمؤسسات والمعاهد غير الحكومية.	61,857
العدد الكلي للطلبة الملتحقين في الجامعات والمؤسسات والمعاهد الحكومية.	1,750,507
العدد الكلي للطلبة الملتحقين في الجامعات والمؤسسات والمعاهد غير الحكومية.	1,858,550

المصدر: *Ameri,2014*.

لا بل توجه عدد لا بأس به من الشباب الإيراني للالتحاق بالجامعات الموجودة في خارج البلاد، (بلغ عددهم 38,380 طالباً عام 2010 حسب إحصائية منظمة اليونسكو)[8]. ويمكن أن يعزى هذا الأمر الى ازدياد التنافس بين الطلبة المتقدمين للتخصصات العلمية الطبية والهندسية المتميزة في الجامعات مما يدفع العائلات الى تحمل نفقات إرسال أولادهم للدراسة خارج البلاد. وتستأثر الجامعات الأمريكية، والكندية، والبريطانية، والألمانية والماليزية باهتمام الطلبة الذين يرومون الدراسة الجامعية خارج البلاد ـ أنظر الجدول (1 - 13).

الجدول (1 - 13) ـ أعداد الطلبة الين أكملوا الدراسة الجامعية خارج البلاد خلال السنوات 2008-2010.

السنة	المراتب الأولى للجهات الدراسة التي يقصدها الطلبة الإيرانيون					المجموع
	1	2	3	4	5	
2010	ماليزيا 6,588	الولايات المتحدة 4,689	بريطانيا 3,163	ألمانيا 2,745	كندا 2,364	38,380
2009	الولايات المتحدة 3,475	ماليزيا 3,475	بريطانيا 2,849	ألمانيا 2,561	كندا 2,086	31,542
2008	الولايات المتحدة 3,063	ماليزيا 2,442	بريطانيا 2,400	ألمانيا 2,231	أوكرانيا 1,780	26,927

المصدر: http://wenr.wes.org/2013/04/wenr-april-2013-an-overview-of-education-in-iran/

[8] . حصلنا على هذه المعلومات من الموقع:
http://wenr.wes.org/2013/04/wenr-april-2013-an-overview-of-education-in-iran/

وبذلك تكاثرت أعداد الملتحقين بمؤسسات التعليم العالي، والمتخرجين منها فبلغت أعدادهم أرقاماً بكبيرة باتت تشكل أزمة ضخمة حيث، لم تعد فرص العمل في بلد محاصر، قادرة على استيعابهم، فعّمت البطالة، بين أفراد هذه الشريحة، وأضحت الحكومة قبالة مأزق جديد.

وانصبغت إيران نتيجة لهذه التخمة في أعداد مخرجات التعليم العالي، وعدم وجود بيئة عمل مستقرة، بارتفاع أعداد العقول المهاجرة من البلاد، بحثاً عن فرص للعمل، بحيث احتلت إيران، وبجدارة !، المرتبة الأولى، على صعيد نزيف العقول، حيث يهاجر منها سنوياً، حوالي 150,000 من حملة الشهادات الجامعية بحثاً عن فرص عمل في خارج البلاد.

2 . 3 . 1 . 4 . هيئات ومراكز البحث العلمي في إيران:

في بداية عام 2003، صادق المجلس الأعلى للثورة الثقافية في إيران على مقترح مجلس الباحثين العلميين في إيران ووجه بإنشاء المجلس الوطني للعلوم *I.N.S.F* لدعم الحركة العلمية في عموم إيران، وتنظيم أنشطة البحث العلمي، وترسيخ قاعدة علمية متينة ومستدامة، داعمة لأنشطة البحث والتطوير ونشر العلوم بالبلاد. ويتمتع هذا المجلس باستقلالية عن المؤسسة الحكومية، بينما تمول انشطته بواسطة مؤسسات حكومية، ومنح من المصارف، وهيئات من القطاع الخاص، بالإضافة الى التمويل الذاتي من الخدمات والمشورة العلمية والتقنية التي يوفرها للغير.

ويعمد هذا المجلس الى توفير مختلف أشكال دعم أنشطة البحث والتطوير التي تلتحق بقائمة أولويات وحاجات البلاد بناء على ما يتضمنه ضمن الكتاب الذي يصدره سنوياً المجلس الوطني للبحث العلمي *N.S.R.C* (*Wikipedia,2015*).

ولضمان تحقيق أهداف المجلس، وفرت إدارته دعماً مالياً ومعنوياً، سخياً، للعاملين على برامج البحوث العلمية والتقنية، سواء كانت إقامتهم داخل إيران، أو خارجه، لترسيخ بيئة حاضنة لأنشطة عملية وتقنية رصينة.

وبدأ المجلس بترسيخ مبدأ حماية الملكية الفكرية للنتاج العلمي للعاملين معه عن طريق التنسيق مع الهيئات المحلية والدولية، لتغطية متطلبات حماية حقوق الملكية الفكرية وتسجيل براءات الاختراع، مع منح حصص للباحثين من العوائد المالية التي يمكن أن تتحقق عن تطبيق نتائج الابتكار على أرض الواقع.

وأنشأت الحكومة الإيرانية مؤسسة النخبة الوطنية بإيران *INEF* في النصف الأول من عام 2005 بعد أن صادق المجلس الأعلى للثورة الثقافية في إيران على نظام المؤسسة على أن تدار بصورة مباشرة بواسطة نائب رئيس الجمهورية.

وتهدف هذه المؤسسة الى رعاية ودعم النخب الوطنية، التي يحق لها الالتحاق بالمؤسسة متى امتلكت قدرات عملية ومعرفية، وقدرة على الابتكار المتميز، سواء من داخل المؤسسات الأكاديمية، أو خارجها. ويعد أعضاء هذه المؤسسة من العلماء والباحثين النخبويين الذين يساهمون في رسم مسار، حاضر ومستقبل، التنمية العلمية والتقنية لإيران (*Wikipedia,2015*).

وتمنح لأعضاء هذا المجلس تسهيلات سخية، سواء على شكل منح مالية، أو دعم وطني لاستكمال مشاريعهم البحثية، مع استثنائهم من الخدمة العسكرية، ومحددات السفر، وغيرها من القوانين التي قد تحد من نشاطهم وتنقلهم

داخل البلاد وخارجها. وبحسب وكالة أخبار فارس في عام 2014، فقد بلغ عدد أعضاء المجلس 13,000 عضواً، حصل فقط 72 شخصية منهم على لقب عالم، بينما عد بقية الأعضاء ذوي مواهب متميزة، أو ذكاء فارق.

من جهة أخرى، ترتبط المؤسسة الإيرانية للعلوم والتقنية *IROST* بوزارة العلم والبحث والتقنية في إيران منذ إنشائها في عام 1980 بقرار من المجلس الثوري الإيراني. وتعد هذه المؤسسة أكبر مركز للبحث العلمي في عموم إيران، والذي يركز جل اهتمامه نحو تطوير الاستراتيجيات، والسياسات الوطنية، مع رعاية نظم البحث العلمي، وإدارة وتشكيل الرؤية التي تسترشد بها بقية مؤسسات ومراكز البحث العلمي، والتقني في عموم البلاد.

ولهذه المؤسسة تعاون وثيق مع كثير من المؤسسات والمنظمات الدولية مثل: UNESCO[9]، WIPO[10]، UNDP[11]، COMSTECH[12]، COMSATS[13]، TWAS[14]، ISESCO[15]، IFIA[16]، APCTT[17]، IOR-ARC[18].

إضافة الى المؤسسات والمنظمات البحثية الوطنية، آنفة الذكر، تتوفر مراكز أخرى للبحث والتطوير (59 مركز)، تستقر معظمها بالعاصمة طهران، وتتوزع حقول اختصاصاتها بين: مراكز بحوث طبية (17 مركز)، ومراكز بحوث علوم صرفه (13 مركز)، ومراكز بحوث هندسية وتقنية (12 مركز)، ومراكز بحوث إنسانية (6 مراكز)، ومراكز بحوث اقتصادية (4 مراكز)، ومراكز بحوث تربوية وتعليمية (3 مراكز)، مراكز بحوث علوم سياسة واجتماع (مركزين)، ومراكز بحوث معلوماتية (مركزين).

2 . 3 . 1 . 5 . دور الحكومة في دعم نظام التعليم:

تعد الحكومة الإيرانية من الأنظمة السخية (في منطقة الشرق الأوسط، وعموم الدول النامية بحجم التخصيصات التي توفرها كل عام من موازنتها الاستثمارية) على صعيد تلبية النفقات التي تتطلبها عملية التعليم في إيران (*John&Aytng,2011*).

ويبدو واضحاً من الجدول (1 - 14) أن إيران قد خصصت نسبة تتراوح 15-21 % من الانفاق الحكومي لدعم أنشطة نظام التعليم المختلفة بالبلاد خلال السنوات 2000-2011، بيد أن الضغط على النفقات بسبب الحصار الاقتصادي على البلاد قد أجبر الحكومة على تخفيض النسبة، لكنها لا زالت تشكل نسبة عالية مقارنة مع بقية بلدان المنطقة.

---

[9] . منظمة الأمم المتحدة للتعليم والثقافة والعلوم.
[10] . المنظمة العالمية للملكية الفكرية.
[11] . برنامج التنمية الإنمائية للأمم المتحدة.
[12] . منظمة المؤتمر الإسلامي للتعاون العلمي والتقني.
[13] . هيئة العلوم والتقنية للتنمية المستدامة في دول الجنوب.
[14] . الأكاديمية العالمية الثالثة للعلوم.
[15] . المنظمة الاسلامية للتعليم والثقافة والعلوم.
[16] . جمعيات المخترعين الدولية.
[17] . مركز نقل التقنية في آسيا.
[18] . الجمعية الهندية للتعاون الإقليمي.

الجدول (1 - 14) ـ حصة نظام التعليم من الانفاق الحكومي خلال السنوات 2000-2012.

المؤشر	2000	2006	2011	2012
الموازنة الحكومية العامة، مليار ريال.	124,796	597,743	1,175,286	1,000,000
الناتج الإجمالي المحلي، مليار ريال.	574,693	2,000,000	6,104,868	6,757,090
نسبة الناتج الإجمالي المحلي من التمويل العام.	21.7 %	29.3 %	19.3 %	15.7 %
الانفاق الحكومي على التعليم، مليار ريال.	26,493	107,283	175,496	…
نسبة نفقات التعليم من الناتج الإجمالي المحلي.	4.6 %	1.7 %	2.9 %	…
نسبة نفقات التعليم من التمويل العام.	21.1 %	17.9 %	15.0 %	…

المصدر: *M.O.E,2015*.

وتتراوح نسبة الانفاق الحكومي على النظام التعليمي بين 3-5 % من الناتج الإجمالي المحلي. وتتألف المبالغ المخصصة للنظام التعليمي من المبالغ المخصصة: المبالغ المخصصة لمؤسسات التعليم العام والخاص، والميزانية التشغيلية لإدارات المؤسسات التعليمية، مع مبالغ دعم للطلبة، وأخرى لجهات تشترك بعملية التعليم، مثل: أنشطة البحث والتطوير، وتدريب الكوادر البشرية، وغيرها من النفقات ـ انظر الجدول (1 - 15).

الجدول (1 - 15) ـ تفاصيل نسب الانفاق الحكومي على النظام التعليمي في إيران خلال السنوات 2000-2011.

المؤشر	2000	2006	2011
نسبة الانفاق على التعليم العام من الانفاق الحكومي الكلي.	16.0 %	13.6 %	10.2 %
نسبة الانفاق على التعليم العالي من الانفاق الحكومي الكلي	3.9 %	3.4 %	4.1 %
نسبة الانفاق على التعليم غير النظامي من الانفاق الحكومي الكلي.	1.2 %	0.9 %	0.7 %
نسبة الانفاق على التعليم العام من الناتج الإجمالي المحلي.	3.47 %	3.99 %	1.96 %
نسبة الانفاق على التعليم العالي من الناتج الإجمالي المحلي.	0.8 %	1.00 %	0.78 %
نسبة الانفاق على التعليم غير النظامي من الناتج الإجمالي المحلي.	0.27 %	0.30 %	0.10 %
نسبة الانفاق العام على التعليم من الناتج الإجمالي المحلي.	4.61 %	5.29 %	2.84 %
نسبة الانفاق على التعليم من الانفاق الحكومي الكلي.	21.1 %	17.9 %	15.0 %

المصدر: *M.O.E,2015*.

وتستأثر مراحل التعليم الأساسي بحصة الأسد من التمويل في حين لا يظفر التعليم العالي الا بنسبة تتراوح بين 0.8 – 1.0% من الناتج الإجمالي المحلي.

بيد أن هذه المبالغ الكبيرة لم تعد تفي بمتطلبات العملية التعليمية نتيجة للتوسع الكبير في حجم أنشطة التعليم، وزيادة حجم الطلبة، الأمر الذي انعكس على دخل كوادر التدريس التي استمرت منذ عام 2006 باحتجاجاتها في مدن مختلفة بسبب انخفاض أجورها، وتفشي الفساد الإداري والعلمي الذي بات يطول مؤسسات التعليم العالي الخاص، فتراجعت الجودة بمخرجات التعليم بشكل ملحوظ، ولم تعد كفة الجودة راجحة مع كفة الكم الكبير للملتحقين بالمدارس والجامعات والمعاهد والمتخرجين منها.

2 . 3 . 1 . 6 . واقع نظام التعليم والتحديات القائمة:

تشخص امام النظام التعليم الإيراني، بشقيه الأساسي، والعالي، الكثير من التحديات التي تتقارب بسماتها، الى حد كبير، مع طبيعة التحديات التي تكتوي بها نظم التعليم في بلدان المنطقة، وبالخصوص الدول العربية. ويستثنى من ذلك حزمة من التحديات الإضافية التي قد تنشأ عن الضغط المستمر الذي تمارسه المرجعية الدينية للثورة الإيرانية، والتي تحاول أن تعمّق من الصبغة العقدية بالكثير من مفردات ومناهج التعليم، وممارسات التدريسيين، والطلبة على حد سواء.

لكن ما يشد الاهتمام أن الخطاطة العقدية للثورة الإيرانية، لم تؤثر على حق الأنثى بالتعليم، لذا فإننا نلاحظ حضوراً مميزاً للإناث، في جميع مراحل التعليم، مع تقارب قد يرتقي الى مستوى التطابق على صعيد القدرة على القراءة والكتابة لدى الجنسين، الأمر الذي يؤكد غياب التفرقة بفرص التعليم بسبب الجنس في عموم مراحل وقطاعات النظام التعليمي بإيران.

2 . 3 . 1 . 7 . العقبات والتحديات التي تواجه التعليم الأساسي:

رغم إطراد النمو الكمي في قطاع التعليم الأساسي بإيران، مع سعي الحكومة الى تطوير مناهجه، وطرائقه، وزج تقنيات الحاسوب، وانتشار خدمة الانترنيت في الكثير من المدارس بمراحلها المختلفة، فلا زالت هناك كثير من العقبات والتحديات التي تعاني منها المؤسسة التعليمية بحسب تقارير تقييم أداء هذه المرحلة من عملية التعليم، والتي ذكرتها وزارة التربية الإيرانية في تقاريرها التي أعدت لمراجعة واقع وتحديات التعليم بإيران عام 2015 (*M.O.E,2015*).

ويمكن إجمال أهم التحديات التي أشار اليها التقرير بما يأتي:

- ✓ فشل النظام التعليمي في بلوغ الأهداف التي أدرجت ضمن الخطة الخمسية 2009-2014 للتعليم الأولي بإيران، مع استمرار تراجع أعداد الطلبة الملتحقين بالمدارس الابتدائية، أو ضمان استبقائهم للالتحاق بالمراحل التعليمية اللاحقة.
- ✓ تدار جلّ تفاصيل العملية التعليمية بإشراف حكومي مباشر، مع غياب الموارد غير الحكومية، يصاحبها شحة الموارد الحكومية بسبب الظلال التي تصاحب الحصار المفروض على إيران منذ سنوات.

- ✓ ارتباط المناهج بالخطاطة العقدية والسياسية للنظام مع تغييب صبغة التنوع الذي تتسم به الثقافة الإيرانية الخصبة، فأصبح المنهج احادياً ولا يتوافق مع حاجات التعليم المفتوح في عصر المعلومات والمعرفة.
- ✓ عدم توظيف تقنيات التعلّم والتعليم التفاعلية والاعتماد بصورة كلية على نهج التصاق المدرس والطالب كلياً بالكتاب المنهجي.
- ✓ تباطؤ عمليات توظيف تقنيات الحاسوب وأدوات المعلومات والاتصالات وزجها في العملية التعليمية.
- ✓ شعور الكادر التدريسي بعدم الرضا نتيجة تراجع دخولهم، وصعوبة العيش، الأمر الذي ينعكس سلبياً على تفرغهم وإقبالهم على تعليم طلبتهم.
- ✓ عدم اعتماد الأساليب الحديثة لإدارة أنشطة إدارات المدارس، وكوادرها التدريسية، وغياب التنسيق فيما بينهم على صعيد تقويم الأداء، أو التعاون مع أولياء أمور الطلبة.
- ✓ استمرار المدارس بنهج العمل بصورة شبه مستقلة، مع غياب التواصل بين الإدارات، والكوادر التدريسية، مع بقية المدارس في المحافظة ذاتها، أو بقية المحافظات لتطوير العملية التربوية، وتنمية مهارات الكوادر التدريسية.

2 . 3 . 1 . 8 . العقبات والتحديات التي تواجه التعليم العالي:

تتجه الأنظار، دوماً، نحو التعليم العالي (الجامعي) بوصفه مفتاحاً جوهرياً، وأداة أساسية لبناء القدرات المعرفية لدى جيل الشباب، وتطوير إمكاناتهم على ممارسة أنشطة البحث والتطوير، وتثوير مكامن الابتكار لدى أفراد هذه الشريحة لبلوغ مستوى رصين من القدرات والمهارات التي تدعم استمرار أنشطة مجتمع المعلومات، وتواكب التطورات المفاهيمية والتقنية التي تسري في كيانه السيبراني.

بيد أن التصاق المناهج وطرق التدريس بأطر ثابتة وغير متطورة بشكل يتناسب مع متطلبات مجتمع المعلومات والمعرفة، والتكيّف مع متطلباته بات يشكل عقبة أمام تحقيق هذا المرحلة من التعليم في ممارسة دوره الحقيقي في إنتاج جيل يتمتع بقدرات ومهارات تؤهله للتوطن في الفضاء الجديد لمجتمع المعلومات وترسيخ قدراته التنافسية في بيئة رقمية، باتت تعجّ بالابتكار والنمو المستدام.

من أجل هذا لم تعد مؤسسات التعليم العالي الحكومية قادرة على توفير التمويل الكافي لتوفير بيئة التعليم العالي التي تمتلك القدرة على بناء قدرات معرفية تتوافق مع مطالب مجتمع المعلومات وسوق العمل الملتحق بمنتجاته وخدماته.

وإذا كانت مؤسسات التعليم العالي قد نجحت في تخريج عدد كبير من الاختصاصات الطبية والهندسية، فإنها لم تفلح في إنتاج قاعدة معرفية رصينة في قطاع العلوم الإنسانية والاجتماعية، والعلوم الطبيعية، رغم تكاثر عدد الجامعات وتنوّع الفروع العلمية فيها. وقد عزى رئيس الجمهورية حسن روحاني، هذه الظاهرة، الى الخطوط الحمراء التي قد رسختها المؤسسة الدينية والسياسية خلال العقود التي خلت، بحيث أجبرت الإدارة الجامعية، والطلبة على توجيه اهتماماتهم الأكاديمية خارج نطاق هذه الخطوط، من أجل هذا يلاحظ تراجع مرتبة النتاج العلمي الإيراني في حقول المعرفة الطبيعية بحيث لم تنجح باللحاق بدول مثل: السعودية، وسنغافورة، ومصر، وتركيا (*Jawad,2014*).

2 . 3 . 1 . 9 . جودة النظام التعليمي:

أولاً: جودة التعليم الأساسي:

تعد جودة التعليم الأساسي من المعايير المهمة لتقييم أداء النظام التعليمي، والبرهنة على مستوى تحقيقه للأهداف التربوية التي تهدف المؤسسة التعليمية الى تحقيقها من خلال ممارسة تفاصيل العملية التعليمية على الطلبة الملتحقين بأروقة مراحلها المختلفة.

وقد تزايد اهتمام المنظمات الدولية والوطنية بمراجعة وتقييم جودة مدخلات النظم التعليمية ومخرجاتها، مع الحرص على مراجعة وتحليل المناهج والبيئة التعليمية الحاضنة للطلبة لضمان حصولهم على مستوى رصين من المعرفة التي تدعم قدرتهم على التواصل مع المجتمع، من خلال تطوير مهاراتهم، وتعزيز مساهمتهم بالمجتمع الذي ينتمون إليه. وقد تبنت منظمة اليونيسيف مجموعة من المعايير لتقييم جودة التعليم الأساسي توزعت مؤشراتها على خمسة محاور أساسية (*UNICEF,2000*): مستوى جودة معيشة الطلبة والرعاية الصحية التي توفرها الدولة لهم، وجودة عناصر البيئة التعليمية، وجودة محتوى المناهج التعليمية، وجودة العمليات التربوية التي تمارس داخل أروقة مراحل التعليم المختلفة، واخيراً جودة الصبغة المعرفية والمهارات التي تنجح المؤسسة التعليمية بمنحها لطلبتها بعد إنهاء حضورهم فيها.

وأظهرت عملية المراجعة التي قامت بها وزارة التعليم الإيرانية (لما تم تحقيقه في المراحل الدراسية المختلفة لنظامها التعليمي) وجود ثغرات كبيرة على صعيد مستوى أهداف الجودة التي حاولت بلوغها خلال السنوات 2000-2014، والتي تجلت من خلال (*M.O.E, 2015*):

- ✓ عدم استكمال الوزارة لعملية إنشاء أنموذج معياري لتطوير مختلف عناصر الجودة في النظام التعليمي، وبمراحله المختلفة، وبقيت محاولات الارتقاء بالجودة تتسم بالفردية، مع محدودية تأثيرها.
- ✓ لا زالت الكثير من المؤسسات التنفيذية بعيدة عن التواصل والتناغم مع التغييرات الجذرية التي تبنتها وزارة التعليم في السنوات الأخيرة.
- ✓ غياب التوزيع المتوازن للموارد التعليمية على صعيد الرقعة الجغرافية، أو المؤسسات التربوية، أو المراحل الدراسية، مما عمّق الفجوة وشكّل عقبة امام خطط الارتقاء الشامل بالجودة.
- ✓ عدم كفاية المبالغ المخصصة لعمليات الارتقاء بالجودة.
- ✓ ممانعة الكثير من الجهات التنظيمية لعملية التغير داخل حدود النظام التعليمي، الأمر الذي يثبط عملية الإصلاح بشكل كبير.

ورغم هذه العقبات (التي قد تشترك في كثير منها إيران مع الدول العربية) فقد نجحت وزارة التربية بإيران في الارتقاء بكثير من عناصر محاور الجودة الخمسة (آنفة الذكر)، منها: تبني معايير لمساحة القاعات الدراسية، زيادة نسبة المستوى الأكاديمي للكوادر التدريسي بنسبة بلغت 7 %، زيادة بنسبة 10 % على صعيد تطوير المناهج الدراسية، زيادة حصة مشاركة القطاع الخاص بنسبة 20%. ولا زالت وزارة التربية الإيرانية تبذل كل ما في وسعها للارتقاء بجودة التعليم والايفاء بالأهداف التربوية التي وضعتها مؤسسة *EFA* لضمان جودة التعليم الأساسي في دول العالم المختلفة.

ثانياً: جودة التعليم العالي:

صاحب النمو المتسارع في عدد الطلبة الملتحقين بالمؤسسات الجامعية، ضمن الدراسات الأولية والدراسات العليا، حصول تراجع ملحوظ في جودة التعليم العالي مع انحسار مستوى المادة العلمية التي يتلقاها الطلبة داخل أروقة هذه المؤسسات. من أجل هذا فقد دعا رئيس الجمهورية حسن روحاني (في اجتماع له مع رؤساء الجامعات وعمداء الكليات، وإدارات معاهد البحوث) الى الموازنة بين النمو الكمي، مع الحفاظ على مستويات جودة التعليم العالي والبحث العلمي في البلاد (*Jawad,2014*).

من جهة أخرى تحوّلت الكثير من الجامعات الخاصة من مؤسسة اكاديمية باتجاه مؤسسة ربحية، تمنح الشهادات الجامعية الأولية والعليا مقابل مبالغ نقدية، تتزايد قيمتها بحسب ارتقاء مستوى الشهادة الأكاديمية، دون أن تولي اهتماماً بالرصانة العلمية، بحيث توجهت الكثير منها الى قبول الطلبة دون امتحان اختبار، مع تحديد الفرع العلمي بحسب المبلغ الذي يسدده الطالب الملتحق بمؤسسة التعليم الأهلي، كذلك بدأت ظاهرة كتابة الأطروحة العلمية لكثير من طلبة الدراسات العليا، خارج نطاق المؤسسة الأكاديمية، وبواسطة مكاتب متخصصة، وبأثمان باهضة (*Jawad,2014*).

ويلاحظ تفاوت المستوى العلمي بين الجامعات الحكومية والخاصة، حيث أظهر المسح الأكاديمي الذي قام به مركز العالم الإسلامي للتنويه العلمي *Islamic World Science Citation Center* (*ISC*) أن جامعة طهران تتبوأ المرتبة الأولى، بين بقية الجامعات الإيرانية، وتليها جامعة شريف للتقنية، ثم جامعة أمير كبير للتقنية. وقد نجحت هذه الجامعات الثلاث بالحصول على موطئ قدم في التراتبية العولمية للجامعات، في حين بقيت بقية الجامعات الإيرانية بعيدة عن المراتبية العلمية ـ العولمية[19]. ولم تولي الإدارة الحكومية الإيرانية اهتماماً لهذه المعايير العولمية، وأكدت أنها تحتل المرتبة الثالثة على صعيد رقي المستوى العلمي في الجامعات بعد اليابان وتركيا (*Wikipedia,2015*).

لقد بلغ سوق العمل، في إيران، مرحلة التخمة بالشهادات الجامعية، مع تراجع فرص العمل المتوفر لأعداد الخريجين، التي باتت تتزايد يوماً بعد، في ظل حصار اقتصادي خانق، انبسطت ظلاله على عموم المشهد الاقتصادي بالبلاد.

وقد نشب عن هذه التخمة غير المتوازنة زيادة نسبة عدد حملة الشهادات الجامعية ممن يعانون البطالة، والتي ارتفعت من 0.44 % في عام 1976 الى 19.40 % في عام 2011، وهي نسبة عالية. بيد أن هذه التخمة قد منحت البلاد فرصة زيادة عدد سنوات الدراسة لدى موظفي القطاع الحكومي والخاص في عموم إيران، الأمر الذي منح المؤسسة الإيرانية فرصة احتضان كوادر بشرية تتناسب مرحلة تعليمها مع متطلبات العمل.

وقد انصبغت نسب بطالة خريجي التعليم العالي في إيران، بصبغة الواقع، والذي تناقض في كثير من مفرداته مع مشهد سوق العمل في بقية بلدان المنطقة، بسبب الحصار وتراجع أنشطة التصنيع والانتاج. فازدادت نسبة البطالة

[19] . تبوأت جامعة طهران مرتبة بين أفضل 401–500 جامعة وفق نظام التقييم العولمي للجامعة ***Academic Ranking of World Universities*** لعام 2013[19].

في الاختصاصات العلمية (الهندسة 22 %، علوم الحياة 26 %، علوم الحاسب 30 %)، بينما تتضاءل هذه النسبة في الاختصاصات الإنسانية والاجتماعية التي لم تتجاوز 11 %[20].

وبالوقت ذاته فإن طلبة الدراسات العليا الجامعية لم يسلموا من مشكلة البطالة، بعد أن تزايد أعداد الخريجين من مرحلتي الماجستير والدكتوراه، بحيث بلغ عدد العاطلين منهم، عن العمل في عام 2014 حوالي 52,000 خريج جامعي (*Habibi,2014*) ـ أنظر الجدول (1 - 16).

الجدول (1 - 16) ـ مساهمة الموارد البشرية في إيران بسوق العمل مع نسب البطالة لدى خريجي التعليم العالي 1976-2011.

السنة	العدد الكلي لخريجي التعليم العالي (العاملين والعاطلين)	مساهمة القوى العاملة			نسبة البطالة
		العاملة	العاطلة	المجموع	
1976	433,391	286,315	11,365	297,680	0.40 %
2011	10,011,676	3,741,999	901,619	4,643,618	19.40 %
متوسط النمو السنوي	9.40 %	7.60 %	13.3 %	8.2 %	...

المصدر: ***Habibi,2014***.

2 . 3 . 1 . 10 . السعي الى إصلاح النظام التعليمي:

أولاً: الإصلاحات في نظام التعليم الأساسي:

تتبنى وزارة التعليم الإيرانية جملة من الخطط التي تسعى الى إحداث إصلاحات جذرية في النظام التعليمي، مع ضمان بلوغ الأهداف الدولية لمنظمة *EFA* لضمان تحقيق سلسلة من القفزات النوعية. ومن هذه الإصلاحات: تطوير مستويات الخدمات التعليمية التي تقدمها مؤسساتها المختلفة للطلبة، حث المدارس على وضع خططها السنوية التربوية والتي تتوافق مع أهداف الوزارة مع إجراء مراجعة فصلية لما تقق من الأهداف، حث القطاع الخاص على الدخول في ساحة النظام التعليمي للارتقاء بمستوياته، تطوير أدوات ومعايير التقويم التربوي لبلوغ قيم حقيقية للمؤشرات التربوية، توسيع دائرة استخدام أدوات المعلومات والاتصالات في العملية التربوية، وتطوير المناهج ومحاولة زج مفردات إثرائية في مضامينها، السعي الى تطوير التعليم المهني لتوفير فرص عمل لشريحة واسعة من الطلبة الذين لا تتوفر امامهم فرص الالتحاق بالتعليم الجامعي.

وتبقى هذه الأهداف، وغيرها من الأهداف التي لم نعرّج عليها، حبيسة للواقع الإيراني، والتجاذبات السياسية مع المعسكر الغربي بشأن الملفات العالقة، وملفات أخرى تفرضها المرجعية الدينية (بين الحين والآخر) بناء على خطاطتها العقدية والسياسية في التعامل مع المفردات والأدوات التي تدخل الى إيران من المعسكر الغربي. بيد أن المؤشرات التقليدية تظهر أن هناك تطور ملموس على صعيد الإصلاحات التي تتبناها وزارة التعليم، غير أن جلّ هذه الإصلاحات

[20] . سبق وأن ذكرنا أن التعليم العالي في قطاع العلوم الإنسانية والاجتماعية لا زال محدوداً في إيران بالمقارنة مع الفروع العلمية. الأمر الذي أدى الى زيادة الطلب على هذه الاختصاصات، مقابل التخمة بالاختصاصات العلمية وتراجع الطلب عليها في سوق العمل.

لا زالت قاصرة عن توفير المناخ المناسب لتطوير وبناء قدرات كافية للالتحاق بالمعايير التي تفرضها عملية الانتماء الى مجتمع المعلومات والمعرفة المعاصر.

2 . 3 . 1 . 11 . الدور الذي يمارسه نظام التعليم في تشكيل مجتمع المعلومات بإيران:

لقد نجح نظام التعليم الإيراني بتحقيق قفزات نوعية على مستوى رفع المستوى العلمي، وتعميق المهارات، والخبرات، لدى شريحة واسعة من مخرجاته خلال العقود الأخيرة. بيد أن إيران شأن بقية دول المنطقة، لم تفلح في تحقيق توازن معرفي على عموم الرقعة الجغرافية للبلاد.

كما أن النظام التعليمي لم يستطع تجاوز العقبات والتحديات التي انغرزت في أرض الواقع، ولا زالت بنيته التحتية، وموارده، ومدخلاته، ومخرجاته لا ترقى الى مستوى المعايير التي تسود في مجتمع المعلومات والمعرفة المعاصر.

بيد أن النظام الإيراني قد نجح في إنشاء مجموعة من البؤر العلمية والتقنية، نتيجة لاستثمار الخبرات المتراكمة لعدة أجيال من حملة الشهادات العليا، والخبراء الإيرانيين، واحتضان الموارد البشرية المتميزة، وبناء القدرات داخل حدود إيران، وخارجها. وقد أنتجت هذه البؤر نتاجاً علمياً وتقنياً ارتقى بها الى مرتبة الدول المتقدمة في مجالات متعددة.

من اجل هذا يمكننا القول أن نظام التعليم في إيران قد نجح في إذكاء حركة علمية وتقنية ناشطة لدى مجموعة من البؤر العلمية والتقنية المنتشرة هنا وهناك، بحيث رسخت منتجاتها الأكاديمية والتقنية حقيقة انتماء هذه النواتج وتوافقها مع منتجات مجتمع المعلومات، بيد أن هناك الكثير من الفجوات العلمية، والتقنية، والتنظيمية، التي تقف عائقاً امام إلحاق مجتمع إيران بأكمله مع ركاب مجتمعات المعلومات والمعرفة المعاصرة.

وسنحاول أن نتوقف عند بعض الشواهد التي تؤكد حصول تطور علمي وتقني في إيران، وبمستوى يرقى بها الى مصاف لم تبلغها دول المنطقة العربية، بحيث باتت تشكّل منافساً صعباً لجارتها تركيا في هذا المضمار.

2 . 3 . 2 . تطوير القدرة على استثمار أدوات المعلومات والاتصالات:

تنسق الإدارة الحكومية في إيران، والقطاع الخاص مع الجامعات الإيرانية ومعاهد التعليم العالي لإعداد دورات متنوعة على صعيد بناء القدرات في مضمار تقنية المعلومات وهندسة المعلومات والاتصالات.

بلغ عدد الملتحقين بهذه الدورات والبرامج التدريبية عام 2007 حوالي 95,800 متدرب، مع متوسط نمو سنوي للالتحاق بهذه الدورات بلغ حوالي 80% (*Davarinejad&Saffari,2011*).

بصورة عامة بلغ عدد الطلبة الملتحقين في أقسام تقنية المعلومات والحاسب في الجامعات الحكومية عام 2007 (دون الأخذ بعين الاعتبار طلبة كل من جامعة بايمي نور وجامعة آزاد) حوالي 108,700 طالباً (بلغت نسبة العنصر النسوي 49 %). وقد التحق منهم حوالي 45.5% في برامج الدبلوم العالي، بينما التحق حوالي 52.8 % ببرامج درجة البكالوريوس، والتحق 1.7 % منهم ببرامج الحصول على درجة الماجستير والدكتوراه. بالمقابل يبلغ عدد المتخرجين في اختصاصات تقنية المعلومات والاتصالات والاختصاصات ذات الصلة بها حوالي 20,000 طالب سنوياً (*Davarinejad&Saffari,2011*).

وإضافة الى الزيادة الكبيرة في عديد كوادر طلبة الدراسات الجامعية، والمعاهد العليا، وحملة الشهادات العليا في تخصصات تقنيات المعلومات والاتصالات، فيمكن تقييم النتائج المتحققة على أرض الواقع بمضمار تطوير قدرات المواطنين الإيرانيين على استخدام أدوات المعلومات والاتصالات، وتوظيفها بشكل مقبول في فضاء إقامتهم بمجتمع المعلومات المستحدث من خلال مراجعة المعايير التالية:

المعيار الأول: مؤشرات الوصول الى أدوات المعلومات والاتصالات:

تعد بوابات الاتصالات والمعلومات المتمثلة بأعداد المشتركين بشبكات الهواتف الأرضية والمحمولة، وأعداد المشتركين بخدمة الانترنيت مؤشراً على مقدار وصول المواطنين الى الخدمات الاتصالية والتواصلية في مجتمع المعلومات. كما يؤشر مقدار سعة الخدمة المتوفرة للمواطن على مستوى الفعاليات التي يمكن أن يمارسها المواطن أثناء حضوره في فضاء مجتمع المعلومات السيبراني.

ويمكن تقييم قدرة المواطن الإيراني على الوصول الى الفضاء السيبراني من خلال مراجعة بيانات الجدول (1 - 17).

الجدول (1 - 17) ـ مؤشرات الوصول الى أدوات المعلومات والاتصالات واستخداماتها في إيران لعام 2015.

المؤشر	التفاصيل
نسبة المشتركين بخدمة الهواتف الأرضية.	37.66 %
عدد المشتركين بخدمة الهواتف الأرضية.	30,818,440
نسبة الهواتف التي تعمل بخدمة الدفع المسبق.	0.2 %
نسبة القرى التي تتوفر فيها شبكات الهواتف المحمولة.	71.7 %
نسبة المواطنين الذين تشملهم تغطية شبكات الهواتف المحمولة.	94.2 %
عدد خطوط الهواتف المحمولة المسجلة.	137,602,325
عدد خطوط الهواتف المحمولة المفعّلة.	71,142,413
نسبة تفعيل بطاقات الهواتف المحمولة.	92.25 %
عرض حزمة الإنترنيت العولمي لكل مستخدم.	17 kb/sec
عدد محطات الستالايت.	17,211
عدد المشتركين بخدمة ADSL العريضة.	6,229,639
طول شبكة الألياف الضوئية ـ الإيرانية.	56,466 Km
عدد المشتركين بخدمة WIMAX العريضة.	1,212,603
عدد المشتركين بخدمة انترنيت الهواتف المحمولة GPRS.	22,753,375
عدد المشتركين بخدمة انترنيت الهواتف المحمولة 3G.	7,081,918
نسبة الاشتراك بالخدمة العريضة (الثابتة والمحمولة).	19 %
عدد القرى التي تتوفر فيها مراكز خدمة انترنيت نشطة.	10,030

المصدر: ***I.I.S.,2015.***

ويبدو واضحاً أن خدمة الهواتف المحمولة قد مدّت نسيج شبكاتها على مساحة واسعة من البلاد (نسبة المواطنين الذين تشملهم التغطية 94.2 %)، كما أن هذه الخدمة قد غطت أكثر من 70 % من القرى الإيرانية.

بالمقابل يلاحظ أن نسبة انتشار خدمة الانترنيت العريضة لا زالت متراجعة بالمقارنة مع تركيا ودول الخليج العربي، حيث لم تتجاوز نسبة 19% من حجم المشتركين بالخدمتين الثابتة والمحمولة والتي نجم عنها (مع تراجع حصة المواطن من سعة خدمة الانترنيت) تراجع كبير على صعيد إتاحة الفرص أمام المواطن بالمشاركة العريضة في التطبيقات والخدمات التي تتوفر ضمن بيئة الانترنيت.

المعيار الثاني: مؤشرات استخدام أدوات المعلومات والاتصالات:

يمكن استثمار قيم مؤشرات استخدام المعلومات والاتصالات في المجتمع الإيراني لتحديد مستوى الاقبال على توظيف هذه الأدوات، والتي تؤشر بجلاء على حضور قدرات رقمية تشجّع على هذا الإقبال.

ويلاحظ من بيانات الجدول (1 - 18) أن عدد مستخدمي الانترنيت في إيران، في زيادة مستمرة خلال السنوات الأخيرة (نسبة النمو خلال السنوات 2013-2015 قد بلغت حوالي 52 %). من جهة أخرى يلاحظ أن نسبة الوصول الى خدمة الانترنيت من المساكن لا زالت منخفضة حيث يفضل المواطن الإيراني على الوصول اليها من خلال جهازه المحمول، أو من مقاهي الانترنيت، أو أمكنة أخرى.

وفي كل الأحوال يلاحظ تراجع استخدام الانترنيت على المستوى العولمي في كل من: المؤسسة التربوية، وقطاع التجارة والأعمال (بنوعيه *B2B+B2C*)، ويمكن أن يعزى ذلك الى ارتفاع كلفة الخدمة بالمقارنة مع دول الجوار، مع تراجع حصة المواطن من سعة الانترنيت بحيث لا تلبي حاجاته من استخدامها.

الجدول (1 - 18) ـ مؤشرات استخدام أدوات المعلومات والاتصالات والانترنيت في مجتمع المعلومات الإيراني.

مؤشر الاقبال على الاستخدام في إيران	نزعة الاستخدام خلال السنوات 2015-2013		
	2013	2014	2015
حجم استخدام الانترنيت في إيران، مليون مستخدم.	21.0	26.0	31.4
الوصول الى الانترنيت في القطاع السكني.	20.8 %	26.5 %	35.8 %
القدرة على الوصول الى المحتوى السيبراني*.	4.0	3.9	…
القدرة على الوصول الى الانترنيت في المدارس*.	2.9	2.7	2.7
استخدام الانترنيت في قطاع التجارة والأعمال ـ *B2B**.	3.9	3.7	3.6
استخدام الانترنيت بين قطاع التجارة والمستهلكين *B2C**.	3.6	3.5	3.6
تأثير تقنيات المعلومات والاتصالات على المنتجات والخدمات الجديدة*.	4.1	3.9	3.8
نسبة الموارد البشرية التي تعمل في قطاع المعرفة.	15.0 %	15.0 %	16.0 %

المصدر: *Bilbao-Osorio, et.,al.,2014, Dutta, et.,al.,2015*.

(* تتراوح قيمة المؤشر بين 0-7 وبصورة تصاعدية)

المعيار الثالث: المهارات الفردية بتقنيات المعلومات والاتصالات:

لا يمكن لمؤشرات القدرة على الوصول الى أدوات المعلومات والاتصالات، أو مؤشرات استخدام هذه الأدوات أن تحدد كفاءة ونجاعة برامج بناء القدرات ما لم تراجع مؤشرات المهارات الفردية التي يتمتع بها المواطن الإيراني، والتي يمكن من خلالها ان نحدد مسارات الاستخدام ومستويات كفاءة الحضور في فضاء مجتمع المعلومات السيبراني.

ويبدو واضحاً من بيانات الجدول (1 - 19) أن جلّ المهارات التي يمتلكها عامة المواطنين الإيرانيين في هذا المجال تصب في التعامل المبسط مع البيئة البرمجية للحاسب (تنصيب، وخدمات الملفات ـ 15-62%)، واتقان استخدام البرمجيات المكتبية وإرسال البريد الالكتروني لحد ما (18-27 %).

الأمر الذي يؤكد فرص ممارسة المواطن الإيراني لسلوك مواطن تقليدي في بيئة مجتمع المعلومات، بيد أن مستويات الحضور السيبراني لا زالت بدائية ولا ترقى الى مستويات حضور يناظر المهارات الفردية التي يتمتع بها أفراد الدول المتقدمة.

الجدول (1 - 19) ـ المهارات الفردية بتقنيات المعلومات والاتصالات لدى المواطن الإيراني.

المهارة بتقنية المعلومات والاتصالات	نسبة المواطنين الذين يمارسونها
تنصيب أدوات المعلومات والاتصالات.	15 %
البحث عن البرمجيات وتنصيبها.	31 %
كتابة برنامج واستخدام اللغات البرمجية.	4 %
إرسال البريد الالكتروني ومرفقاته.	27 %
نقل الملفات والمجلدات السيبرانية.	23 %
نقل الملفات بين الحاسب وبقية أدوات المعلومات.	62 %
اتقان استخدام البرمجيات المكتبية.	18 %
استخدام الدوال الرياضية في الصحائف الممتدة.	9 %

المصدر: *M.o.ICT,2015*.

2 . 3 . 3 . مستويات التطور السيبراني في المحافظات الإيرانية:

لا شك ان هناك ثمة تباين كبير بين مستويات التطور السيبراني التي تمتلكها مختلف المحافظات الإيرانية نتيجة لوفرة ورصانة البنية التحتية للمعلومات والاتصالات المتوفرة فيها، ومستوى تطور مواردها البشرية، ووجود عوامل داعمة للتطور السيبراني نتيجة لوجود مؤسسات تعليم عالي، أو مؤسسات بحثية، أو منشآت صناعية تسهم في دعم عجلة تطور محافظة دون غيرها، إضافة الى نشاط بيئتها الاقتصادية التي تنعكس على التطور السيبراني.

لقد صنفت وزارة تقنية المعلومات والاتصالات الإيرانية المحافظات الإيرانية، بحسب مستويات التطور السيبراني الى ثلاث مراتب (ضعيفة، متوسطة، وممتازة) ـ أنظر الجدول (1 - 20).

ويبدو أن من مجموع 31 محافظة إيرانية، هناك خمس محافظات قد تسنمت مرتبة تطور رقمي ممتازة، بينما بلغ عدد المحافظات ذات المستوى المتوسط سبع عشرة محافظة، بينما هناك تسع محافظات لا زالت مستوى التطور السيبراني فيها ضعيفاً.

الجدول (1 - 20) ـ مرتبة التطور السيبراني لمختلف المحافظات الإيرانية ـ عام 2015.

المحافظة	عدد السكان	عدد المساكن	عدد القرى المرتبطة بأدوات المعلومات والاتصالات	مؤشر تطور أدوات المعلومات والاتصالات	المرتبة التطور السيبراني للمحافظة
أذربيجان ، الشرقية.	3,787,837	1,163,851	2,634	5.05	متوسطة
أذربيجان، الغربية.	3,170,346	897,253	3,079	4.53	متوسطة
أردبيل.	1,271,337	363,373	1,682	4.51	متوسطة
أصفهان.	4,981,829	1,557,834	1,572	5.40	متوسطة
البورز.	2,512,997	790,129	*	6.21	ممتازة
عيلام.	570,494	146,305	529	4.93	متوسطة
بوشهر.	1,079,899	271,928	564	5.36	متوسطة
طهران.	12,463,954	3,985,415	1,118	6.584	ممتازة
بختياري.	914,949	252,070	702	4.45	ضعيفة
خراسان، الجنوب.	752,503	193,835	1,669	4.56	متوسطة
خراسان، رازاوي.	6,192,260	1,846,567	3,233	4.71	متوسطة
خراسان، الشمال.	888,764	259,324	774	4.09	ضعيفة
خوزستان.	4,663,404	1,221,547	2,834	4.92	متوسطة
زنجان.	1,039,062	309,772	878	4.63	متوسطة
سمنان.	652,096	197,959	474	5.86	ممتازة
سيستان.	2,670,911	640,910	4,788	3.48	ضعيفة
فارس.	4,686,015	1,351,102	3,390	5.13	متوسطة
قزوين.	1,229,114	378,363	821	4.96	متوسطة
قم.	1,197,245	347,371	152	5.43	متوسطة

المحافظة	عدد السكان	عدد المساكن	عدد القرى المرتبطة بأدوات المعلومات والاتصالات	مؤشر تطور أدوات المعلومات والاتصالات	المرتبة التطور السيبراني للمحافظة
كردستان.	1,518,821	430,945	1,603	4.43	ضعيفة
كرمان.	3,030,622	860,831	4,634	4.36	ضعيفة
كرمنشاه.	1,959,291	568,720	2,427	4.46	ضعيفة
كوهجيلويه.	681,864	169,133	1,662	4.48	ضعيفة
جوليستان.	1,845,946	529,129	1,005	4.48	ضعيفة
جيلان.	2,515,891	825,954	2,498	5.06	متوسطة
لورستان.	1,790,694	497,726	2,375	4.35	ضعيفة
مازندران.	3,134,102	997,527	2,974	5.75	ممتازة
ماركازي.	1,443,297	454,719	1,036	5.08	متوسطة
هرمزجان.	1,647,796	438,038	1,334	5.11	متوسطة
همدان.	1,779,028	541,220	1,085	4.57	متوسطة
يزد.	1,049,860	332,721	794	5.74	ممتازة
المجموع	77,122,228	22,821,769	54,320	....	

المصدر: *I.I.S.,2015*.

3 . دور أدوات المعلومات والاتصالات في منظومة الاقتصاد الإيراني:

انصبغ الاقتصاد الإيراني بصبغة الاقتصاد الريعي نتيجة للثروات النفطية الهائلة التي تمتلكها البلاد، بيد أن هذا الأمر لم يمنع من توجهات جادة نحو تنويع الموارد نتيجة لوجود اقتصاد زراعي، وصناعي نشط في البلاد أسهم الى حد كبير بمد منظومة الاقتصاد الإيراني بموارد اقتصادية جمّة.

وقد تنبهت الإدارة الحكومية الى أهمية التنوّع بعد أن أثقل الحصار الذي فرضته الولايات المتحدة والمعسكر الغربي على إيران نتيجة الخلافات التي نشأت نتيجة لتداعيات الملف النووي. الأمر الذي حتّم على الحكومة الإيرانية إعادة ترتيب عناصر منظومتها الاقتصادية وزيادة حصص القطاعات الإنتاجية للتعويض عن تراجع مركبة الاقتصاد الريعي التي تراجع حضورها في المشهد الاقتصادي الكلي للبلاد.

ولما كان حجم سوق المعلومات الاتصالات في إيران، يغطي حاجات بضعة وسبعون مليوناً من المواطنين الإيرانيين فقد فرض على الجهات التخطيطية والمؤسسات الصناعية والاقتصادية التفكير في تنشيط المركبة الاقتصادية لأدوات المعلومات والاتصالات، على المستويين التقني والخدمي لتوفير قيمة اقتصادية مضافة الى المشهد الاقتصادي الكلي للبلاد، وتخفيض كلف استيراد الأدوات والخدمات من خارج البلاد.

3 . 1 . مراجعة سريعة للمشهد الاقتصادي الإيراني:

يحتل الاقتصاد الإيراني المرتبة الثانية في منطقة الشرق الأوسط وشمال أفريقيا بعد السعودية، وبناتج إجمالي محلي ناهز 406.3 مليار دولار عام 2014. وتحتل ايران المرتبة ذاتها على مستوى عدد السكان بعد مصر، بعد أن ناهز عدد سكانها 80.8 مليون نسمة بحسب المسح السكاني في شهر تموز من عام 2014 (*WB,2015*).

ولا زال الاقتصاد الإيراني منصبغاً بسمة الاقتصاد الريعي، ويستمد مناهله من الموارد الهيدروكربونية (المرتبة الثانية على صعيد احتياطي الغاز الطبيعي، والمرتبة الرابعة على صعيد احتياطي النفط الخام)، مع حضور متواضع للإنتاج الزراعي وتغطية الإنتاج الصناعي والخدمي لجل الاحتياجات المحلية، مع تصدير بعض المنتجات المصنعة لدول الجوار.

ورغم الاستراتيجية الاقتصادية التي تبنتها الحكومة في محاولة لإصلاح البيئة الاقتصادية للبلاد في خطتها الخمسية الأخيرة (2011-2015) فلا زال اقتصاد البلاد يعاني من آثار الحصار العولمي، بحيث لا زال الاقتصاد الإيراني مقيماً في المرتبة 130 من بين 189 دولة على صعيد نشاط بيئة الأعمال(*WB,2015*).

ورغم الضغوط الكبيرة التي فرضها الغرب على إيران، كنتيجة حتمية للخلاف حول النشاط النووي الإيراني، فقد نجح هذا الاقتصاد بتحقيق نمو اقتصادي بلغ 3.0% في عام 2014، بالمقارنة مع الانكماش الذي بلغ 1.7 % عام 2013 بعد أن برزت نتائج التطور على صعيد تصدير جزء من غلة الإنتاج الزراعي ومنتجات صناعية الى بلدان المنطقة (ارتفعت نسبة التصدير من هذه المنتجات عام 2015 بنسبة 24.2 % عما تحقق في عام 2014) (*WB,2015*).

من جهة أخرى لا زالت ظاهرة البطالة تلقي بظلالها القاتمة على المشهد الاقتصادي للبلاد بعد أن بلغت نسبتها في الوثائق الحكومية الى 10.3 % في عام 2013، بينما تؤكد منظمات المجتمع المدني أن هذه النسبة قد ناهزت 20 %.

وقد نجم عن شحة فرص العمل، توجّه الكثير من الشباب نحو الهجرة، بحيث تفيد الاحصائيات أن ما يقارب 150,000 شـ اب إيراني من خريجي المدارس العالية يهاجرون من البلاد بحثاً عن فرص للعمل في دول الخليج أو أوربا. بالمقابل تسعى الحكومة الى توفير 8.5 مليون فرصة عمل خلال السنتين القادمتين لضمان تقليص نسبة البطالة مع بداية عام 2016 الى 7 %.

ولا زال خط الفقر يشخص أمام عدد كبير من المواطنين الإيرانيين الذين يقدر عددهم بمقدار 4.5 مليون مواطن (4 % -6 % من عدد السكان).

ورغم بوادر الاتفاق النووي بين إيران ومجموعة الدول 5+1، فإن استمرار انخفاض أسعار النفط، مع التخمة التي تعاني منها السوق العالمية قد ينشب عنها استمرار النمو المتواضع بالمشهد الاقتصادي في إيران بحيث لن تتجاوز نسبته من 0.6 % الى 1.5 % خلال السنتين القادمتين، مع احتواء لنسبة التضخم بحدود قد لا تتجاوز 17.3 %(*WB,2015*).

3 . 2 . دور قطاع الصناعة البرمجية:

تعد إيران من البلدان الرائدة في استخدام البرمجيات بمنطقة الشرق الأوسط، فقد وظفت حزمة متنوعة من البرمجيات في جامعاتها وبعض مؤسساتها الحيوية منذ بداية العقد السابع من القرن العشرين، وعمدت الى استيراد أجهزة حوسبة مع استقدام خبراء من خارج البلاد لتوطين التقنية الجديدة في البلاد (*Soofi&Ghazinoory,2013*).

وبعد أن وطدت الثورة الإسلامية أركانها في البلاد، وأعيد فتح الجامعات مع بدايات عام 1983، أعيد النظر في مسألة البرمجيات ووجهت الإدارات العلمية اهتمامها نحو استنطاق الحاسب باللغة الفارسية لضمان استبعاد آفة الغرب عن الآلة التي بدأ سلطانها بالنمو التدريجي، وتعمقت الحاجة اليها في إدارة الكثير من الأنشطة العلمية والتنظيمية بالبلاد. وقد توسع دائرة الطموح عند المؤسسات الحكومية فنوقش مبدأ تطوير صناعة البرمجيات في إيران، كخطوة أولى نحو التوجه الى تصدير البرمجيات لدول المنطقة، وبلدان العالم الثالث. بيد أن الانشغال بتداعيات الحرب العراقية ـ الإيرانية قد أسهمت في إرجاء الخطط الأولية للتطوير في قطاع الصناعة البرمجية، واجبرت أصحابها على الرضا باستبقائها على الرفوف التي حوت الكثير من المشاريع الإيرانية الطموحة خلال تلك الحقبة الزمنية.

في بداية الثمانينات من القرن العشرين قامت الحكومة الإيرانية بتشكيل المجلس الإيراني ـ الأعلى للمعلوماتية *The Iranian High Council of Informatics* لحل الإشكاليات التي نشأت مع الشركات الأجنبية، وبعد أن قامت الكثير من الشركات مثل: *IBM, NCR* بتجميد أنشطتها التقنية والتجارية في البلاد. وهيمن الكساد على قطاع صناعة البرمجيات خلال العقد ذاته، وافتقدت الكثير من مؤسسات المعلومات والاتصالات الى أي نوع من الدعم الحكومي (*Nicholson &Sahay,2003*).

وبقي قطاع الحوسبة الطرفية *Mainframe Computing* يعاني من عزلة تقنية لحين دخول الحواسب الشخصية الى البيئة الإيرانية في بدايات عام 1985.

وقد شـهد عهد رئاسة محمد خاتمي تحولاً جزئياً باتجاه إعادة تنشيط الدور الذي يمارسه قطاع الصناعة البرمجية، بعد أن توجهت الإدارة الحكومية نحو الانفكاك من قبضة الاقتصاد الريعي المرتكز بالكلية الى الموارد النفطية، والرغبة بالسير على طريق الالتحاق بمجتمع الشبكات السيبرانية، بيد أن هذا التحول لم يكتب له سوى نجاح جزئي، نتيجة للضغوط التي مارستها المؤسسة الدينية المهيمنة على الكثير من القرارات السياسية والتنظيمية في إيران.

تعد كل من شركة *Magfa*، وشركة *Iran Info-Tech Development* المنبثقتين عن المؤسسة الأم، مركز تطوير تقنية المعلومات *IDRO* من الشركات الحكومية ـ الرائدة بمضمار الصناعة البرمجية في إيران. وتأتي من بعدهما شركة *Hamkaran System* والتي تعد من اكبر شركات القطاع الخاص بقطاع الصناعة البرمجية. وهناك شركات أخرى نجحت في ترسيخ حضور تطبيقاتها في سوق البرمجيات الإيرانية، مثل: *Sena Soft*، *Dadeh-Paradazi*، *Iran Argham*، *Information Network*، *Kafa System*، *Iran system*، *Puya* (*EIU,2004*).

وقد استثمرت الكوادر البرمجية الإيرانية، ما يتسم به نظام التشغيل *Linux* في دعم البرمجيات ذات المصادر المفتوحة *Open Source Programs* من خلال سعي حثيث لإصدار نسخة مطورة تدعم اللغة الفارسية، وتدعم المبرمجين في إنشاء تطبيقات بعيدة عن الهيمنة التقنية التي تمارسها بيئة تشغيل *Microsoft Windows*. وفي الوقت ذاته بدأت توجهات نحو إنتاج برمجيات حماية وصيانة أمن المعلومات الوطنية بالظهور، بيد أنها قد بقيت بعيدة عن منال

السوق المحلية بعد أن حرصت الإدارة الحكومية على التزام الكتمان بصددها لضمان مسألة الأمن السيبراني الوطني الإيراني بعيداً عن خصومها السياسيين في المنطقة والمعسكر الغربي (*Khaksar&Khaksar, 2015*).

وأسهم إغفال الحكومة الإيرانية عن مسألة قرصنة البرمجيات في إعراض شركات البرمجيات العالمية عن تسويق برمجياتها في السوق الإيراني، لعدم وجود عقوبات رادعة لعمليات القرصنة، كما نجم عن ذلك التأثير بصورة مباشرة على الابتكار في هذا القطاع، بعد أن غابت حقوق الملكية الفكرية لأصحاب التطبيقات الجديدة من المبرمجين الإيرانيين، وعدم اهتمام المستثمرين بتنمية هذا القطاع الحيوي.

فانحسر نشاط الصناعة البرمجية عن ساحة نشاط القطاع الخاص، وتركز نشاطها في دائرة القطاع الحكومي لتلبية حاجات آلة الصناعة العسكرية، والتطبيقات الصناعية التي حظر المعسكر الغربي على إيران تطوير تقنياتها، وتطبيقات أمن المعلومات وخوادم الانترنيت، والشبكات المحلية.

من أجل هذا أحيطت أنشطة الصناعة البرمجية في إيران بالسرية والكتمان، وأضحت ملفاتها جزءاً لا يتجزأ من الملفات التي لا تروم إيران الإفصاح عن الكثير من تفاصيلها. لذا لا تكاد تعثر على شركات برمجيات ـ إيرانية قد حاولت الحصول على ترخيص *ISO9000* أو ترخيص قدرات أنموذج النضج *Capability Maturity Model-SEI2002* وذلك للإبقاء على نشاطاتها بعيداً عن أنظار الغير، والعمل وفق مواصفات تلبي حاجات القطاع الحكومي.

وقد شكلت حاجات القطاع الحكومي الى البرمجيات حوالي 70 % من مجموع حجم الطلب عليها في السوق الإيراني، وذلك لتلبية الاحتياجات الخاصة برقمنة محتوى الأرشيف الحكومي، وإدارة دفة الكثير من الأنشطة التي لم يعد من الممكن توجيه دفاتها بصورة سليمة دون استخدام الحواسب ومن خلال تطبيقات برمجية فاعلة (*Nicholson &Sahay,2003*). من أجل هذا فإن صحوة قطاع صناعة البرمجيات في إيران قد ارتبط، الى حد كبير، بتلبية احتياجات مؤسسات الدولة والقطاع الحكومي، مضافاً اليه احتياجات قطاع الصناعات المدنية والعسكرية المتخصصة، بالإضافة الى تطبيقات لضمان أمن وسلامة بيئة شبكات المعلومات وتحصينها من الاختراق المحتمل نتيجة الارتباط بخدمة الانترنيت.

تعد مجموعة *FarsiTEX* الجهة الإيرانية الرائدة على صعيد زج اللغة الفارسية في تطبيقات البرمجيات مفتوحة المصدر. حيث أثمرت جهود كوادرها التقنية في إضافة اللغة الفارسية الى برنامج *TEX* الذي يعد من تطبيقات سطح المكتب الشهيرة *Desktop Publishing Application* في منصة البرمجيات مفتوحة المصدر.

ابتدأت المجموعة عملها في بدايات عام 1992 داخل أروقة مركز الحوسبة في جامعة شريف للتقنية *SUT*، ثم تلتها محاولات أخرى في عام 1999 لزج اللغة الفارسية في تطبيقات أخرى، والتي مهدت لظهور مجموعة جديدة وجهت اهتمامها صوب تطوير حضور اللغة الفارسية في مواقع الويب، والتي أصبحت تعرف بمجموعة *FarsiWEB* لدى العاملين على صعيد تطوير البيئات البرمجية الناطقة باللغة الفارسية (*Tabesh, et. ,al., 2004*).

وتقبل بعض المؤسسات الحكومية والمصارف الإيرانية ومعظم شركات تجهيز خدمة الانترنيت على استخدام خوادم البيئة البرمجية لنظام *Linux*، بينما اتجهت الكثرة الكاثرة من مستخدمي الحواسب الى خوادم نظام تشغيل بيئة *Microsoft Windows* وعلى التوازي مع نظام *Linux*.

لقد استشعرت الإدارة التقنية الإيرانية الى أن نظام *Linux* وتطبيقاته ذات المصدر المفتوح أضحت جزءاً لا يتجزأ من البنية التحتية الداعمة للتطبيقات الفارسية، بعد أن أصبح الحصار التقني واقعاً مفروضاً على البلاد، وتوجه الحكومة المحموم باتجاه تطوير برامجها التي لا تتوافق مع رغبات المعسكر الغربي. لقد أصبحت العلاقة بين التطبيقات البرمجية الوطنية وهذا النظام علاقة غير قابلة لأي نوع من أنواع الخصام او الفصام. لذا أصبحت هذه البيئة مفتاحاً لتنمية صناعة برمجية وطنية شاملة، وتوجهت أنظار جميع المراكز والمؤسسات نحو تطوير الحضور الإيراني في هذه البرمجية لحماية المنجزات والتطبيقات الوطنية، من جهة، وتخفيف آثار طوق الحصار التقني في مجتمع بات يرتكز الى الفضاء السيبراني بكثافة.

في ظل هذه التوجهات، اقترح مركز التقنيات المتقدمة للمعلومات والاتصالات *AICTC* في جامعة شريف للتقنية تطوير نسخة فارسية لنظام *Linux* في بداية عام 2001، والذي لم يتردد المجلس الأعلى للثورة الاسلامية في إيران على المصادقة عليه بالسنة ذاتها. وقد اوكلا الإدارة التقنية للمشروع، للمركز البحثي ذاته بعد أن بوشر بالمشروع على أرض الواقع في عام 2003.

وقد أسهم هذا المشروع في ولادة خمسة مشاريع جديدة وجهت اهتمامها نحو إثراء وتطوير مكتبات أساسية لبرمجيات داعمة للمشروع تغذي حضور اللغة الفارسية وتعمّق حضورها بشكل متوافق مع التطبيقات الوطنية. ولدت هذه التطبيقات في عام 2003 ثم لم تلبث أن ظهرت ثمان تطبيقات داعمة للغة الفارسية في عام 2004 كانت نتاجاً لمشاريع جديدة حاولت سد الثغرات المصاحبة لحضور اللغة الفارسية في بيئة برمجية لم تصمم لحضورها المكثف الذي اقتضته السياسة البرمجية الجديدة في إيران (*Tabesh, et. ,al., 2004*).

وقد باركت الإدارة الحكومية، هذه الإنجازات الوطنية، ولقيت استحساناً كبيراً لدى القطاع الأكاديمي ومؤسسات البحث العلمي، وفي قطاع التجارة والأعمال الذي توفرت له فرصة توظيف بعض أنماط التعاملات السيبرانية في بيئته التي تعاني من الحصار.

وبحلول عام 2002، بلغ عدد الشركات السيبرانية المسجلة، في عموم إيران، حوالي 1,200 شركة، تخصصت 200 شركة منها في مضمار الصناعة البرمجية. وقدّر الريع المتحقق من تصدير البرمجيات المحلية بحوالي 50 مليون دولار في عام 2008 مرتفعاً الى حوالي 400 مليون دولار بحلول عام 2014 (*Wikipedia,2015*).

لا تكاد تتوفر إحصائيات دقيقة عن عدد العاملين في قطاع الصناعات البرمجية في إيران، بيد أن الكثير من الدراسات الى أن عدد هؤلاء يصل الى حوالي 20,000 مبرمج وتقني من مجموع 150,000 مهندس ومبرمج وتقني يعملون في قطاع المعلومات والاتصالات في البلاد (*Nicholson &Sahay,2003/ IBP,2011*). ويتوزع هؤلاء على حوالي 200 شركة لتطوير البرمجيات تستوطن معظمها (70% من هذه الشركات) بالعاصمة طهران، يعمل فيها حوالي 15% من حجم الموارد البشرية التي تعمل في قطاع الصناعة البرمجية (أي حوالي 3000 مبرمج وتقني من حملة الشهادات الجامعية).

وبدأت تباشير نهوض الصناعة البرمجية في إيران مع خطة تنمية تقنية المعلومات *TAKFA* التي أعدت عام 2003، والتي منحت للمؤسسة الحكومية الدور الحصري في عملية التنمية البرمجية لمجموعة متنوعة من التطبيقات الناطقة

باللغة الفارسية، لتوفير برمجيات تلبي حاجات البلاد ومؤسساتها الحكومية، وقطاع التجارة والأعمال، واحتياجات المواطن الإيراني من تطبيقات تلبي احتياجاته المختلفة.

وقد قام مركز مجلس للبحوث بإيران، في عام 2010، بدراسة لتحديد أهم التحديات التي تقف عائقاً امام تطور صناعة البرمجيات في دول مختلفة، وخرجت هذه الدراسة بتقسيم التحديات الى تسعة مجاميع أساسية. وفي السنة التالية قام المعهد الإيراني لبحوث المعلومات والاتصالات بتخصيص الدراسة السابقة، بعد أن وجه عنايته الى التحديات التي تعاني منها الصناعة البرمجية في إيران (*Khaksar&Khaksar,2015*). ولم تولي هذه الدراسة اهتمامها إلا بصناعة البرمجيات المرتكزة الى بيئة البرمجيات المفتوحة، والتي يشيع استخدامها في التطبيقات المحلية.

وقد ربطت هذه الدراسة التحديات بغياب الدعم المستدام من المؤسسة الحكومية الإيرانية لتنمية وتطوير هذا القطاع الحيوي، ووجود تعارض بين خطط شركات الصناعة البرمجية وتوجهات الحكومة، وغياب التعاون العلمي والتقني مع المؤسسات البرمجية الدولية بسبب الحصار. الأمر الذي جعل التطبيقات الإيرانية مفتقرة الى الدعم التقني، مع غياب البرمجيات المرخصة مما ينجم عنه بين الحين والآخر توقف بيئة التشغيل الداعمة للتطبيقات.

بالمقابل توصل أصحاب التقرير الى قناعة بأن الحصار التقني والاقتصادي على بلادهم قد حوّل وجهتهم نحو البرمجيات ذات المصادر المفتوحة، عمّق معرفتهم البرمجية، بعد الاعتماد الكلي على الخبرات المحلية، فأنتجت برمجيات ذات صبغة محلية، تلبي الحاجات القائمة في قطاعات متعددة، وتحسن النطق والتعامل مع اللغة الفارسية، كما تتسم بانخفاض كلفة إنتاجها، مع تلبية الهاجس الأمني تجاه الاختراقات والثغرات المقيمة في النظم البرمجي الوافدة من البلدان المناوئة، والتي تهيمن على البيئات والتطبيقات البرمجية على حد سواء.

وفي الوقت ذاته لم يعد لمسألة حماية حقوق الملكية الفكرية تأثير ملموس مع البيئة التي انفتحت على جميع المستخدمين، ودون الحاجة الى ترخيص، أو حضور محددات في إعادة تشكيل خوارزميات التطبيقات البرمجية، ومجالات استخدامها.

وقد أصدرت الحكومة الإيرانية مجموعة من القرارات التي اعتنت بمسألة حماية حقوق الملكية الفكرية للبرمجيات المنتجة في قطاع الصناعة البرمجية الوطنية، نذكر منها (*Khaksar&Khaksar,2015*):

- ✓ قانون حماية حقوق منشئ التطبيق البرمجي عام 2000.
- ✓ قانون حماية المحتوى السيبراني للمعلومات عام 2008.
- ✓ قانون الجرائم السيبرانية عام 2009.

بيد أن قناعة مجلس للبحوث في إيران (بنجاعة هذه التشريعات وقدرتها على حماية الصناعة البرمجية في البلاد) تكاد أن تكون شبة معدومة، ولعدة أسباب، منها: عدم وجود فهم سليم لدور البرمجيات وتقنية المعلومات لدى الجهات التشريعية، والقضائية، الأمر الذي لا يوفر فرصة مناسبة لحماية حقوق الملكية الفكرية للشركات البرمجية، كما أن الحكومة لا تولي اهتماماً كافياً بنشاط القطاع الخاص للصناعات البرمجية، الأمر الذي يحول دون وجود دعم كاف لكف عمليات القرصنة، وعدم وجود وعي لدى المستهلك الإيراني بأهمية هه المسألة، وعدم وجود جهات رقابية لحماية حقوق هذه الشركات.

وتشير الدراسات الاقتصادية الى أن الصناعة البرمجية ـ الإيرانية قد بدأت بتحقيق قيمة اقتصادية مضافة بلغت 124.5 مليون دولار خلال السنوات 2001-2009 وذلك من خلال تصدير تطبيقات برمجية متنوعة للناطقين باللغة الفارسية، ممن يقطنون بلدان الخليج العربي، والأميركتين (*Soofi&Ghazinoory,2013*).

وقد توزعت التطبيقات البرمجية الإيرانية بين برامج للإدارة والأعمال، والمحاسبة والإدارة المالية، وبرمجيات تعليمية وترفيهية، وتطبيقات لتصميم مواقع الويب باللغة الفارسية، وإدارة المحتوى السيبراني الفارسي. بالإضافة الى هذه التطبيقات بدأت الإدارة الحكومية بتشجيع قطاع الصناعة البرمجية على إنتاج برمجيات تطبيقية لإدارة عجلة القطاع الصناعي، وإدارة عملية الإنتاج الصناعي، وإدارة الطيران، وقطاعات أخرى باتت تعاني من آثار الحصار التقني الذي فرض على إيران.

3 . 3 . دور قطاع صناعة الحواسب وعتادها وأدوات الاتصالات:

كانت بداية الصناعات الالكترونية في إيران عام 1972 عندما أنشئت مؤسسة إيران للصناعات الالكترونية، وهي مؤسسة حكومية ترتبط بمؤسسة الصناعات الدفاعية، ركزت جل اهتمامها نحو توفير منتجات وخدمات للمؤسسات الحكومية والقطاع الخاص (*Abbasi, et.,al.,2008*). وقد حصل توسع تدريجي في هيكلة هذه المؤسسة بعد أن توسع نقاط أنشطتها التصنيعية والخدمية فضمت خلال مدة قصيرة مجموعة من الشركات الفرعية، نذكر منها: شركة شيراز للصناعات الالكترونية، شركات إيران للاتصالات، ونظم معلومات إيران، وشركات صناعة المكونات الالكترونية، وشركة أصفهان للبصريات، ومركز إيران لبحوث الالكترونيات. وقد بدأت ورش ومصانع هذه الشركات بإنتاج الكثير من المعدات الإلكترونية والاتصالية، مع توفير خدمات داعمة للمؤسسة الحكومية والقطاع الخاص.

ولضمان تكامل بيئة المعلومات الوطنية، وإحكام أمنها، سعت الحكومة الإيرانية الى دعم ورعاية الجهود التي تسعى الى إنتاج الرقاقات الالكترونية، وأدوات المعلومات والاتصالات (الهواتف، وأجهزة البث، وأجهزة الشبكات وملحقاتها)، صعوداً الى إنتاج الحواسب الشخصية، والحواسب العملاقة.

وقد تكاثرت أعداد الشركات الحكومية وشركات القطاع الخاص لإنتاج عتاد الحاسب وأدوات الاتصالات فبلغت حوالي 100 شركة، بيد أن الحكومة لم توجه عناية كافية لتطوير البيئة الحاضنة لهذه الصناعة المهمة، وتوجهت باهتماماتها الى أجهزة محددة تصب في تفاصيل هاجسها المستمر حول حماية الأمن القومي، وتطوير الآلة العسكرية والأمنية الإيرانية. فنتج عن ذلك انكفاء الكثير من الشركات المحلية بسبب غياب الدعم الحكومي، وعدم قدرتها على منافسة بعض المنتجات التي بدأت بالتوفر، تدريجياً، في السوق المحلية.

تعتمد شركات تصنيع الحواسب مبدأ تجميع الرقاقات الالكترونية، والمعالجات المركزية، ووسائط خزن البيانات المستوردة من الصين ومن بلدان جنوب شرقي آسيا، والامارات، والتي توفر حواسب للمستهلك الإيراني بأسعار تقلّ عن الحواسب المستوردة من خارج البلاد. وتوفر الحكومة الإيرانية دعماً مالياً لعمليات البيع من خلال طرح برامج للدفع الآجل، وبواسطة دفعات شهرية تدعم المستهلك للحصول على الحاسب. وقد بلغ حجم الحواسب المنتجة محلياً حوالي 800,000 حاسب سنوياً عام 2004 (*EIU,2004*).

وتقوم ثمان شركات إيرانية بصناعة عتاد الحاسوب والرقاقات الالكترونية بإنتاج مجموعة متنوعة من الأجزاء وعبر شراكات ترخيص مع شركات عالمية مثل: *LG, Samsung, Hyundai, Benq, Tatung, CTX*. حيث تنتج الشركات

الإيرانية شاشات الحواسب، وألواح الحاسب *Motherboards*، لوحات المفاتيح، ومجهزات القدرة *Power Supply*، وفأرة الحاسب *Mouse*، وأنواع مختلفة من البطاقات الالكترونية لتلبية الطلب في السوق المحلية، والتصدير لبعض دول المنطقة. وهناك اتفاقية بين شركة *IDRO* من كوريا الشمالية وشركة *Iran Info-Tech Development* الإيرانية لإنتاج حاسب محلي أطلق عليه اسم *SAHAND* بوشر بتسويقه في سوق أدوات المعلومات بالبلاد.

بلغ حجم إيرادات السوق الإيراني للإلكترونيات (أجهزة الحاسب، والهواتف المحمولة، وأجهزة اللعاب الالكترونية، وأجهزة العرض السمعي البصري) حوالي 7.3 مليار دولار عام 2008، مرتفعاً الى 8.2 مليار دولار في عام 2010. وتتوزع حصص هذا السوق بين 47 % لسوق الحواسب وعتادها الالكتروني، 28 % لسوق الأجهزة المرئية والبصرية، وأخيراً 25 % لسوق الهواتف المحمولة (*Wikipedia,2015*). ويتوقع أن يستمر النمو في حجم هذه السوق بحيث يمكن أن يتجاوز 12 مليار دولار في عام 2015.

3 . 4 . مستويات نضوج اقتصاد المعلومات والمعرفة بإيران:

بات من الضروري لمجتمع المعرفة أن يوطد أركانها داخل حدود فضائه السيبراني، مع السعي الحثيث لإنضاج اقتصاد المعرفة ضمن التعاملات السيبرانية التي تسود بيئته لضمان قدرته على الحضور في المجتمع العولمي الجديد، وفرض ميزته التنافسية في عالم بات يحفل بولادات متتالية لتقنيات المعلومات والاتصالات وادواتها.

ويعد النهج الذي اقترحه البنك الدولي لتحديد مستوى انتشار المعرفة داخل حدود المجتمع، مع بيان المرتبة التي تم بلوغها في ميدان اقتصاد المعرفة مورداً مهماً يمكن اعتماده في دراسة ما تم تحقيقه على المستوى الوطني والإقليمي في هذا المضمار(الرزو،2012).

لقد اتجه برنامج الأمم المتحدة الخاص بتقييم مستويات إدارة المعرفة في مجتمعات بلدان العالم المختلفة الى اعتبار أربعة عوامل رئيسة بوصفها العناصر الرئيسة التي يمكن اعتمادها في تحديد مستوى سعي الاقتصادات الوطنية باتجاه بلوغ مجتمع المعلومات المرتكز في جل أنشطته باتجاه استثمار الموارد المعرفية(*WB,2013*).

وشملت هذه العوامل أربعة محاور جوهرية هي: البنية التحتية للمعلومات والاتصالات، التعليم والموارد البشرية، الابتكار والقدرة التنافسية، وأخيراً نظام الحوافز الاقتصادية التي تسود البلاد.

يقاس مؤشر اقتصاد المعرفة *Knowledge Economy Index* بواسطة أنموذج رياضي يوظف سلسلة من الحسابات التي يقاس من خلالها متوسط قيمة المؤشر لبلد، أو منطقة ما، على أساس قيم متغيرات الأركان الأربعة لاقتصاد المعرفة.

أما مؤشر المعرفة *Knowledge Index* فتعتمد معادلته على قيم متغيرات ثلاثة أركان، بعد استبعاد متغيرات الحوافز الاقتصادية من الأركان الأربعة.

ويبلغ عدد متغيرات الأنموذج 80 متغيراً كمياً ونوعياً، اختيرت بعناية لتصف جميع العوامل المؤثرة على احتساب قيمة مؤشر اقتصاد المعرفة، أو المعرفة في البيئة التي نريد أن نتناولها بالدراسة والتحليل.
وقد حاولنا استقصاء التغيرات الحاصلة في قيم مؤشرات المعرفة واقتصادها في إيران خلال السنوات 1995-2012 وعمدنا الى إدراجها في الجدول (1 - 21).

الجدول (1 - 21) ـ مؤشرات عناصر اقتصاد المعرفة في إيران.

المؤشر	السنة		
	1995	2000	2012
مؤشر اقتصاد المعرفة.	3.59	3.60	3.91
مؤشر تقنية المعلومات والاتصالات.	6.41	5.10	5.28
مؤشر التعليم.	4.47	4.42	4.61
مؤشر الابتكار.	2.86	2.62	5.02
مؤشر نظام الحوافز الاقتصادية.	0.63	2.25	0.73
مؤشر المعرفة.	4.58	4.05	4.97

المصدر: *Knoema,2015*.

ويبدو واضحاً أن مؤشر المعرفة واقتصادها لا زال متراجعاً في ايران قبالة ما تحقق في العالم الغربي، وكذلك بالنسبة لما تحقق في أكثر من دولة بالمنطقة (الأردن: 4.95، الامارات: 6.94، البحرين: 6.90، تونس: 4.56، السعودية: 5.96، عمان: 6.14، قطر: 5.84، الكويت: 5.33، لبنان: 4.56) بينما تفوق مؤشر اقتصاد المعرفة لديها على كل من الجزائر، والسودان، وسوريا، والعراق، ومصر، والمغرب، واليمن (الرزو،2015).

ويبدو أن آثار الحصار الاقتصادي الذي فرضه الغرب على ايران (بسبب برنامجها النووي) قد أسهم في تغييب آثار الخطة الوطنية للنهوض بالاقتصاد المرتكز الى المعرفة فنجحت في الارتقاء بمستويات التعليم العالي، والولوج في ساحة التقنيات المتقدمة، غير أن عدم تكامل مادة نسيج البنية التحتية للمعلومات والاتصالات فيها، مع عدم ترويج استخدام الكثير من الأدوات والتطبيقات السيبرانية، خشية من حصول اختراقات تزيل اللثام عن كثير من الأنشطة التي تمارس داخل حدود النظام، أسهمت في تثبيط الخطة العشرينية (الخطة تمتد لعشرين عام) (*Sawahel, W.,2009*). وكانت النتيجة (بعد مرور بضعة سنوات على المباشرة بالخطة) وجود تراجع ملحوظ في إنتاج السلع والخدمات المعرفية قبالة الإنتاج النفطي وغير النفطي، وعدم قدرة الاقتصاد المعرفي على ترسيخ حضوره في المشهد الاقتصادي الإيراني بعد أن أخفق في توليد قيمة اقتصادية ـ معنوية مضافة للناتج الإجمالي المحلي للبلاد (*Najafi, et.,al.,2013*).

3 . 5 . القيمة الاقتصادية المتحققة عن قطاع تقنية المعلومات والاتصالات:

أظهر المسح الميداني الذي قام به فريق مؤسسة تقنية المعلومات في إيران *I.T.O.* أن هناك حوالي 50,000 شركات تجارة وأعمال (صغيرة، ومتوسطة) تمارس أنشطتها في قطاع تقنية المعلومات والاتصالات قبالة 2,500,000 شركة تجارة وأعمال في عموم إيران، ويعمل بهذه الشركات حوالي 159,103 موظف، أن حصة هذا القطاع من الناتج الإجمالي المحلي لم يتجاوز 2.10% (بلغت حصة المعلومات 0.54%، وحصة الاتصالات 1.56%)، بينما بلغت النسبة المضافة الى القيمة الاقتصادية 2.12% (بلغت حصة المعلومات 0.54%، وحصة الاتصالات 1.58%) وهي نسبة ضئيلة تؤشر بجلاء الى تراجع الدور الذي يمارسه هذا النشاط ضمن المشهد الاقتصادي الكلي لدولة إيران (*ITO,2015*) ـ أنظر الجدول (1 - 22).

الجدول (1 - 22) ـ القيمة الاقتصادية المضافة لتقنيات المعلومات والاتصالات على الناتج الإجمالي المحلي لإيران.

الفقرة	التفاصيل
القيمة الاقتصادية الكلية المضافة الى اقتصاد إيران (مليون ريال).	6,894,651,057
الناتج الإجمالي المحلي لإيران (مليون ريال).	6,956,500,326
القيمة الاقتصادية المضافة لتقنيات المعلومات والاتصالات (مليون ريال).	146,271,055
القيمة الاقتصادية المضافة لتقنيات المعلومات (مليون ريال).	37,051,441
القيمة الاقتصادية المضافة لتقنيات الاتصالات (مليون ريال).	109,219,614
حصة القيمة المضافة لتقنيات المعلومات والاتصالات للقيمة الاقتصادية.	2.12 %
حصة القيمة المضافة لتقنيات المعلومات للقيمة الاقتصادية.	0.54 %
حصة القيمة المضافة لتقنيات الاتصالات للقيمة الاقتصادية.	1.58 %
حصة تقنيات المعلومات والاتصالات من الناتج الإجمالي المحلي.	2.10 %
حصة تقنيات المعلومات من الناتج الإجمالي المحلي.	0.54 %
حصة تقنيات الاتصالات من الناتج الإجمالي المحلي.	%61.5

المصدر: *ITO,2015*.

وبناء على الدراسة التي قامت بها مجلة نظم المعلومات في الدول النامية *EJISDC* فقد بلغت قيمة البرمجيات التي تم تصديرها الى خارج البلاد في عام 2008 حوالي 50 مليون دولار (*IBP,2011*) ـ أنظر الجدول (1 - 23).

الجدول (1 - 23) ـ دور تقنية المعلومات والاتصالات في مشهد الاقتصاد الإيراني.

المتغير	التفاصيل
الناتج الإجمالي المحلي الكلي لإيران، مليون ريال.	6,956,500.3
حصة سلع أدوات المعلومات والاتصالات المصدّرة من الحصة الكلية للتصدير غير النفطي.	0.146 %
حصة استيراد أدوات المعلومات والاتصالات من الاستيرادات الكلية.	6.304 %
نسبة القيمة الاقتصادية المضافة لأدوات المعلومات والاتصالات للاقتصاد الكلي الإيراني.	2.30 %
نسبة القيمة الاقتصادية المضافة لأدوات المعلومات والاتصالات للناتج الإجمالي المحلي.	2.28 %
نسبة القيمة الاقتصادية المضافة لقطاع الاتصالات الى الاقتصاد الكلي الإيراني.	1.55 %

المصدر: *I.T.O.I,2014 & I.I.S.,2015*

وأسهم تراجع الاستثمار في قطاع المعلومات والاتصالات في تحجيم أنشطته المختلفة، وحصرها في نطاق لا يكاد يرقى الى مستوى قادر على تحقيق قيمة اقتصادية ـ مضافة مقبولة. كذلك انعكست هذه الظاهرة على كلف تجهيز خدماتها السيبرانية، بحيث اتسمت بمستويات أعلى من دول المنطقة[21] (*Soofi&Ghazinoory,2013*).

بالمقابل قامت الحكومة الإيرانية بدعم غير مباشر لقطاع الصناعة البرمجية من خلال الطلب المستمر على تطبيقات برمجية تعوض الفجوة التقنية لدى قطاع الصناعة، والنفط، والصناعة العسكرية التي باتت بحاجة ماسة الى تطبيقات برمجية لم يعد العالم الغربي يسمح بوصولها الى إيران بسبب الحصار الذي ورثته نتيجة الخلاف حول ملفها النووي.

يضاف الى ذلك الدعم الذي يوفره مكتب نائب رئيس الجمهورية لشؤون العلوم والتقنية الذي يمّول بسخاء الأنشطة الابتكارية للشركات التي توفر خدمات ومنتجات تدعم المؤسسة الحكومية. كذلك تقوم الحكومة الإيرانية بتوفير الموارد الازمة لتنشيط الابتكار في حدائق تقنية المعلومات والاتصالات الوطنية، ومراكز البحث والتطوير المنتشرة داخل حدود المؤسسات الأكاديمية ومراكز بحوث وزارة تقنية المعلومات والاتصالات، لتوفير بيئة داعمة للمشاريع التي تتبناها الحكومة لضمان تفوقها التقني، ودعم مؤسساتها العسكرية والأمنية، على حد سواء.

وعلى هذا الأساس بدأت توجهات صناعة أدوات المعلومات والاتصالات وخدماتها البرمجية تتحول من قطاع يروم الى تحقيق قيمة اقتصادية مضافة الى قطاع يرتبط مباشرة بتلبية احتياجات لإدامة عجلة التنمية في البلاد، ويساهم في الارتقاء بمستويات الكفاية الأمنية في قطاعات الدفاع، والأمن الوطني، وامن الفضاء السيبراني الذي تعمّق تغلغله في فضاء مجتمع المعلومات الإيراني. الأمر الذي أبعده عن هاجس تحقيق قيمة اقتصادية مضافة مقابل القيمة الأمنية والدفاعية المضافة التي يحققها لعموم مؤسسات مجتمع المعلومات الإيراني الناهض.

4 . علامات النضوج التقني بالقطاع السيبراني في إيران:

بالرغم من الحصار الخانق على إيران خلال السنوات الأخيرة، فقد بذلت الدولة الإسلامية بإيران جهوداً جبارة لتنمية قدراتها العلمية التقنية، في سعيها للتفوق على دول المنطقة، وفرض هيمنتها بأدوات وتقنيات تنتجها كوادرها البشرية، دون أن تلتفت الى الثغرات التي تغزو نسيج المجتمع على الصعيد التقني والاجتماعي، بعد أن تبنت مبدأ تنمية بؤر استقطاب علمي وتقني في مساحات محددة من الأنشطة التي خططت لها بعناية لضمان التفوق بعيداً عن المعايير العولمية التي تعتمد لتحديد الميزات التنافسية، أو الجاهزية الالكترونية، أو تكامل البنى التحتية للمعلومات والاتصالات، وغيرها من معايير تقييم انتماء المجتمعات المعاصرة الى مجتمع المعلومات والمعرفة.

وأثمرت بؤر الاستقطاب في دفع عجلة العلوم والتقنية في إيران بقفزات غير مسبوقة بالمقارنة مع بقية دول المنطقة، وعلى صعيد متوسط النمو والتطور العولمي[22].

---

21 . أورد الباحثان مثالاً على ارتفاع كلفة الخدمة بكلفة تجهيز حزمة الانترنيت بسعة ***1MBps*** والتي قد تكلف المواطن الإيراني ذو الدخل المتوسط، كامل دخله الشهري بينما لا تكلف المواطن التركي سوى **11/1** من دخله الشهري، ونسبة **894/1** من دخل المواطن الياباني.

22 . سنحاول حصر اهتمامنا بحقول العلوم والتقنية التي تصب في بوتقة تقنيات المعلومات والاتصالات، وتطبيقاتها السيبرانية، والتي ترتبط ارتباطاً وثيقاً بهيكلة مجتمع المعلومات بإيران، بينما نترك بقية حقول المعرفة لباحثين يوجهون دفة اهتماماتهم الى النهضة العلمية والتقنية الشاملة في هذا البلد.

وقد حاولنا استقصاء مؤشرات التطور العلمي والتقني في إيران، ذات الصلة بتشكيل بيئة معرفية حاضنة ترسّخ جذور مجتمع المعلومات، وتسهم في دعم أنشطة اقتصاد يرتكز بكثافة الى المنتجات والخدمات المعرفية ـ أنظر الجدول (1 - 24).

الجدول (1 - 24) ـ مؤشرات التطور العلمي والتقني في إيران.

الحقل	المرتبة	التفاصيل
الإنتاج العلمي.	17	أثبت المسح الميداني لمؤسسة Scopus أن الإنتاج العلمي في إيران قد بلغ هذه المرتبة في عام 2012 بعد أن بلغ عدد البحوث المنشورة 34,155 بحثاً متفوقة على السويد وتركيا.
النمو في الإنتاج العلمي.	1	بلغت نسبة النمو في الإنتاج العلمي خلال السنوات 1996-2004 400% بينما جاءت الصين بالمرتبة الثانية وبنسبة 300 %. وقد أكد التقرير الأمريكي المنشور في الولايات المتحدة أن إيران تتبوأ المرتبة الأولى عولمياً على صعيد إنتاج البحوث الهندسية، وبنسبة نمو سنوية استقرت عند 23 %.
مؤشر النمو العلمي.	1	ذهبت مؤسسة Science-Metrix الكندية الى أن إيران قد احتلت المرتبة الأولى بعد حصولها على 14.4 نقطة، بينما جاءت بعدها كوريا الجنوبية والتي حصلت على 9.8 نقطة للمؤشر ذاته.

المصادر: *Wikipedia,2015*، *PTV,2010*، *NS,2011*.

ويمكن تبرير هذه النجاحات بتبني السلطة في إيران، خطاطة عقدية، تؤسس مبدأ الاعتقاد بوجود هجمة شرسة تمارسها الدول المتقدمة على الدول الإسلامية، لمنعها من الظفر بعلوم وتقنيات داعمة لتنمية مجتمعاتها وتطوير بنيتها الاقتصادية، الأمر الذي دعم الخطاب الديني لهذه الخطاطة بالتغلغل في نفوس شريحة واسعة من الشعب الإيراني ودفعهم نحو الحرص على توظيف جميع طاقاتهم العلمية في ترسيخ جذور بيئة تنمية علمية، وتقنية مستدامة، للتخلص من الهيمنة التي يمارسها المجتمع الغربي على بلادهم.

وقد هرع مجموعة من العلماء الإيرانيين المتميزين (عام 2011) وبالتنسيق مع أكاديمية العلوم بإيران، الأكاديمية الطبية الإيرانية على إعداد خطة تنمية علمية طموحة (بلغ عدد صفحات التقرير 51 ألف صفحة) تضمنت اقتراح تنفيذ أكثر من 224 مشروع علمي لغاية عام 2025 لضمان نجاح هذه الخطة التنموية التي ستضمن كفاية علمية وتقنية مستدامة لإيران[23].

ولم تشهد الميزانية الوطنية للبحث العلمي في إيران زيادة على 900 مليون دولار منذ عام 2005 والسنوات التي تلتها، والتي تؤشر الى تخصيص فقط نسبة 0.87 % من الناتج الإجمالي المحلي لهذا النشاط، وهي نسبة تقل 40% عن النسبة التي خصصتها الكثير من الدول الصناعية، والدول الناهضة خلال الحقبة الزمنية ذاتها (*Wikipedia,2015*). بيد أن الإدارة الإيرانية قد خصصت مبالغ ضخمة لتطوير قدراتها في ميادين علمية متقدمة

[23] . يمكن مراجعة إعلان الرئيس الإيراني السابق أحمدي نجاد عن هذه الخطة الطموحة في المقال المنشور على الرابط:
http://www.payvand.com/news/11/mar/1079.html.

مثل: التقنيات فائقة الدقة *Nanotechnology*، والتقنية الحيوية، وتقنيات المعلومات والاتصالات التي تدعم برامجها الوطنية في ضمان هيمنة في المنطقة، ومنافسة المعسكر الغربي وكرد مباشر على الحصار المفروض على البلاد.

ولتوفير بيئة داعمة للتقدم العلمي والتقني في إيران وضعت الحكومة خطة علمية ـ تفصيلية عام 2009 (تمتد لمدة 15 عاماً) دعت الى توسيع قاعدة التعليم العالي في البلاد، وترسيخ أواصر التعاون بين المؤسسة الأكاديمية وقطاع الصناعة للإسراع بتنمية اقتصاد وطني، سيرتكز الى المعرفة ومنتجاتها *Knowledge-based Economy* على أن تلتزم الحكومة بزيادة التخصيص لأنشطة البحث والتطوير من 0.59 % الى 4 % من الناتج الإجمالي المحلي، وترفع تخصيصات التعليم العالي من 5.49 % الى 7 % من الناتج الإجمالي المحلي لإيران.

وقد شجّع اهتمام الحكومة بالبحث العلمي وتطوير الآلة التقنية الإيرانية، مجموعة من الشركات الوطنية التي بدأت بمشاريع صغيرة لم تلبث أن نمت، وصلب عودها، نذكر منها شركة *Parse Semiconductor Co.* التي نجحت في إنتاج حواسب محلية تحوي معالجات بسرعة *32 Bits* في عام 2006، وشركة *CeBit* للبرمجيات التي بدأت بطرح برمجياتها المتخصصة في السوق الإيرانية في العام ذاته[24].

4 . 1 . وفرة شبكات المعلومات الوطنية والمحلية:

لم يتغير موقف الثورة الإسلامية في إيران، ومؤسستها العسكرية المتمثلة بالحرس الثوري الإيراني إزاء حضور شبكة الانترنيت وفضائها المفتوح الذي رفض لديهما بشدة، مع التأكيد على ضرورة الحذر من مزالقه التي قد تشكّل تهديداً للثورة الإسلامية، وتقف عائقاً امام تحقيق أهدافها.

ولقد أكدّ آية الله علي خامنئي، المرشد الأعلى للثورة الإسلامية في إيران، وفي أكثر من لقاء خاص وشعبي، على أن حضور خدمة الانترنيت في الفضاء الاتصالي لإيران يعدّ مظهراً من مظاهر النزاع والمدافعة مع قوى الشر بالولايات المتحدة وأطلق على السجال غير المعلن في الفضاء المتخيّل اصطلاح الحرب الناعمة *Soft War* في إحدى خطاباته المناهضة للغرب في عام 2009(*Rhoads&Fassihi,2011*).

أسهم نجاح الانترنيت وحضورها القاهر على المستوى العولمي، وقدرتها الفريدة على صباغة المجتمع المعاصر بصبغتها السيبراني، على مستوى التقنيات والتطبيقات الاتصالية والتواصلية، في إجبار الحكومة الإيرانية ومنظومتها السياسية والعقدية على الرضوخ لهيمنة وسلطة الفيض السيبراني الهادر. فتجرعت جميع الأطراف كأس الانصياع لهذه الهيمنة المتصاعدة، وأرغمت على القبول الى دخول تطبيقاته، بصورة محدودة، الى بعض المؤسسات العلمية الرصينة في إيران. بيد أن الفضاء السيبراني المتدفق تسلل شيئاً فشيئاً، بحيث بلغ فيضه المواطن الإيراني الذي يقطن الأماكن النائية من البلاد.

ونظراً لاستحالة إمكانية إقناع المؤسسة الإيرانية، أو المواطنين بهجر حزم الخدمات المتكاثرة لشبكة الانترنيت، وتطبيقاتها، أو تغطية بريق فضاءات التواصل الاجتماعي التي شدّت البشرية في كل مكان من كرتنا الأرضية، توجهت الحكومة نحو إنشاء نسيج شبكاتي على المستوى المحلي، يلبي جزء من حاجات المواطن، والمؤسسات الحكومية،

[24] . أنظر: **http://www.bbc.com/persian/science/story/2006/03/060310_fb_me_cebit_iran.shtml**.

وقطاع الأعمال للتقليل من فرص التوغّل المستمر، ولتقليل عدد البوابات المنفتحة على الفيض الشيطاني القادم من ناحية الغرب.

فبرزت شبكات محلية لتلبية حاجات القطاع العلمي والتقني، وأخرى لتغطية قطاعات أخرى، بينما خططت الإدارة الحكومية وبالتنسيق مع المؤسسات المهيمنة على أدوات المعلومات والاتصالات ونسيجها الشبكاتي في البلاد، لإنشاء شبكة انترنيت وطنية، تحاكي خدمات شبكة الانترنيت الشريرة، من خلال شبكة إنترنيت تلتزم بالخطاطة العقدية الإيرانية وبالمبادئ الإسلامية الخالصة.

4 . 1 . 1 . شبكة الانترنيت الوطنية:

منذ عام 2005، وبعد أن تبوأ الرئيس محمود احمدي نجاد منصة الحكم في إيران[25]، عكف خبراء السيبرانية وشبكات المعلومات الإيرانيون على تصميم معمارية شبكاتية تحاكي معمارية الخدمات السيبرانية التي توفرها شبكة الانترنيت، وذلك تلبية لنداء المرجعية الدينية التي حذّرت من السموم المناهضة للعقيدة، التي تستوطن بالكثير من مواقع الانترنيت، من جهة، وللهاجس الأمني الذي حذّرت منه المؤسستين الأمنية والحرس الثوري من الثغرات الأمنية التي يمكن أن يستغلها أعداء الثورة الإيرانية لإجهاض الكثير من برامجها العسكرية والنووية.

خطط للشبكة المحلية العملاقة أن تعمل بمعزل عن الشبكة العنكبوتية العالمية *World-Wide-Web* على أن يستكمل عليها وتنطلق بعملها في بدايات عام 2013، بعد أن خصصت لها ميزانية قاربت مليار دولار أمريكي. كان المشروع عبارة عن محاكاة غير متكاملة للمشروع الذي عزلت بموجبه دولة كوريا الشمالية مواطنيها السيبرانيين عن بيئة الانترنيت التي استخدمتها الولايات المتحدة ضد نظام بيونغ يانغ.

وقد تولى إدارة مشروع الشبكة الوطنية للمعلومات *NIN* الخبير عبد المجيد ريفازي، والذي تبوأ منصب وكيل وزارة تقنية المعلومات والاتصالات الإيرانية، لمدة تزيد على خمس سنوات، بعد ان غادر منصبه الرفيع في إدارة امن الاتصالات الدفاعية والصناعات الالكترونية بالبلاد.

وقد بوشر بتشغيل المرحلة التجريبية الأولى (وبقدرات معلوماتية محدودة) من المشروع في محافظة قم، في بداية عام 2010، بينما بدأ تشغيل المرحلة الثانية في نهاية السنة ذاتها بمحافظة كرمان.

ونتيجة لذلك وجهت الحكومة الى مغادرة جميع مواقع وزارات الحكومة الإيرانية لفضاء الانترنيت والالتحاق بفضاء شبكة الانترنيت الوطنية بحلول شهر سبتمبر من عام 2012[26]. وقد قامت الكثير من المؤسسات الحكومية الإيرانية بتصميم وتشغيل آلات بحث خاصة للعاملين فيها، لدرء لعمليات التلصص التي تمارسها الشركات التي تدير أنشطة آلات البحث العولمية مثل: *Google*، أو *Yahoo*.

ويؤكد الكثير من الخبراء، من داخل إيران، وخارجها، على عدم اكتمال هذا المشروع رغم أن الرئيس السابق نجاد قد أكّد لأكثر من مروة على ضرورة استكمال المشروع ومباشرته بالعمل قبل انتهاء مدة ولايته. وقد عزي التأخير لأسباب

[25] . راجع المقال التالي على الموقع: ***http://www.payvand.com/news/10/oct/1189.*html**.

[26] . راجع الموقع: **http://www.wired.co.uk/news/archive/2012-08/07/iran-offline**.

تقنية، وعقبات فرضتها شحة التمويل بسبب الحصار المفروض على إيران، إضافة الى ان اهداف المشروع قد تجاوزت مدى القدرات والمهارات السيبرانية التي تمتلكها الخبرات الإيرانية بهذا المضمار.

وقد عدّ مسؤول الشؤون الاقتصادية بإيران، علي آغا محمدي، الشبكة الايرانية للانترنيت أنموذجاً حيّاً للشبكة الإسلامية المتوافقة مع روح الشرع الإسلامي ومبادئه الأخلاقية السامية، وأن استخدامها حلال شرعاً ولن تكون فيه أية مخالفة شرعية، كما انها يمكن ان تتوسع لتصبح الشبكة البديلة للمعلومات في بلدان العالم الاسلامي (*Rhoads&Fassihi,2011*).

بالمقابل أعلن آغا محمدي أن هذه الشبكة ستلبي حاجات المواطنين في نيل المعرفة والتواصل فيما بينهم، بينما ستبقى الانترنيت (المحرمة شرعاً!) مستخدمة في إدارة الأعمال المصرفية، ومؤسسات الدولة ووزارتها، وبعض المؤسسات البحثية والأكاديمية.

4 . 1 . 2 . الشبكة الوطنية للمعلومات *NIN*:

لتلبية الضغط المتزايد من المؤسسة الدينية، والمؤسسات الأمنية حول فرص استثمار خدمة الانترنيت لخلخلة المنظومة العقدية للمواطن الإيراني، أو الاضرار بمنظومة الأمن الوطني من أعداء كثر يتربصون بالدولة ومؤسساتها المختلفة، اضطرت الحكومة الى إنشاء شبكة معلومات محلية *Intranet* تمتلك سعة عريضة، وترتكز الى مجموعة واسعة من مراكز البيانات الوطنية والمحلية *Data Centers*. وقد أطلق في إيران على هذه الشبكة اصطلاح الانترنيت الشرعية *Halal Internet* (*Soofi&Ghazinoory,2013*).

ولغرض جذب الشباب الإيراني، وعموم المواطنين السيبرانيين بالبلاد الى هذه الشبكة، وإبعادهم قدر الإمكان عن الجزء الشيطاني المستوطن في الجزء المظلم شبكة الانترنيت، فقد عكفت إدارة الشبكة الوطنية على توفير حزم متنوعة من الخدمات السيبرانية الداعمة والتي تلبي ذوق المواطن الإيراني، فطرحت فيها خدمات مثل: محطات تلفازية *IP-TV*، وشبكات اجتماعية، وخدمات متنوعة للحكومة الالكترونية، وخدمات للتجارة الالكترونية، والتعليم الالكتروني. بدأت الشبكة عملها على نطاق تجريبي في عام 2011، ثم تحولت الى العمل بكامل طاقتها في عام 2012 (*Soofi&Ghazinoory,2013*).

4 . 1 . 3 . الشبكة الوطنية العلمية National Scientific Network:

تتألف الشبكة الوطنية العلمية من النسيج الرابط بين الجامعات ومراكز البحث والطوير العلمي المنتشرة في عموم الرقعة الجغرافية للبلاد، وتعد جزءاً لا يتجزأ من الشبكة الوطنية للمعلومات.

وترتبط بهذه الشبكة جميع قواعد البيانات، والمستودعات السيبرانية التي تتوفر في هذه المؤسسات، حيث تحتوي الشبكة على تطبيق برمجي تبادل للمعلومات يوفر لمستخدميها فرصة الحصول على المعلومات والموارد المعرفية وفق نظام ترخيص بحسب تراتبية المستخدمين، ومستويات الترخيص المناظرة لكل منهم.

وتعد قاعدة بيانات مركز المعلومات والوثائق العلمية *Center for Information & Scientific Documents* من اهم الموارد السيبرانية المهمة التي تضم في مستودعاتها السيبرانية أطروحات الدكتوراه والماجستير، وتقارير مراكز البحوث الوطنية، التي أتيحت لمستخدميها (*Khaksar&Khaksar,2015*).

4 . 1 . 4 . شبكة الحواسب العملاقة: Super Computers Network:

بعد أن استكملت جامعة أمير كبير عملية إنتاج حواسبها العملاقة، عام 2011، ونظراً لما تتسم به هذه الحواسب من قدرة حوسبة غاشمة، باشرت الكوادر التقنية بالتخطيط، وبدء العمل في تنفيذ شبكة وطنية لربط الحواسب العملاقة في بيئة رقمية لها القدرة على معالجة وتحليل المسائل الهندسية والتقنية العلمية المعقدة.

وقد عكف فريق من التقنيين والمتخصصين بالصناعة البرمجية على تطوير بيئة برمجية قادرة على احتضان حزم متنوعة من التطبيقات البرمجية الداعمة للأنشطة البحثية في الجامعات الإيرانية، ومراكز البحوث، بمختلف تخصصاتها، وللشركات الخاصة المتحالفة مع القطاع الحكومي. وقد أثمرت هذه الجهود التقنية المضنية في إنتاج أكثر من 60 حزمة برمجية لتلبية احتياجات الحوسبة المعقدة، ولخدمة البرامج الوطنية على صعيد التطبيقات الهندسية، والتقنيات الدفاعية، والتقنية النووية، والتقنيات فائقة الدقة، وغيرها من التطبيقات التي تدعم نشوء وتطوير التقنيات المتقدمة في إيران.

وقد استخدمت بيئة *Linux* (ذات السمة المفتوحة) في إنشاء هذه البيئة البرمجية، وظهرت عدة تطبيقات برمجية في هذه البيئة، منها: برامج محاكاة عملية الاحتراق في نظم دفع الطائرات والصواريخ (والتي تدعم وتسهم في تطوير الصناعة العسكرية في مجال الصواريخ بعيدة المدى، والطائرات)، تحسين كفاءة منظومات الاحتراق لتقليل نسبة الوقود المستهلك وتقليل تلوث الهواء، والتنبؤ بالأضرار المحتملة على الأجسام نتيجة عمليات الارتطام، لتحسين معايير السلامة في السيارات التي تنتج في إيران، وتطوير خواص المعادن المستخدمة في الصناعات التعدينية، والتنبؤ المناخي، وإجراء حسابات معقدة بمجال تقنيات الفضاء والأقمار الاصطناعية (*Khaksar&Khaksar,2015*)

.4 . 2 . صناعة الحواسب العملاقة:

نجحت إيران (في بداية الألفية الجديدة) بلملمة القدرات الهندسية المتقدمة لكوادرها العاملة بمضمار الحواسب والمعالجات الدقيقة *Microprocessors* فنجحت كوادر مركز بحوث المعالجات الدقيقة فائقة السرعة بجامعة أمير كبير للتقنية في بناء حاسب عملاق عام 2007 قادر على إجراء 860 مليار عملية محوسبة بالثانية الواحدة[27].

وبادرت كوادر جامعة أمير كبير للتقنية بالتحالف مع نخبة من تقنيي جامعة أصفهان للتقنية لإنتاج حاسبين عملاقين في عام 2011 بلغت قدرتهما المحوسبة 34,000 مليار عملية محوسبة بالثانية الواحدة[28]. وقد احتل الحاسب العملاق الجديد مرتبة ضمن أسرع 500 حاسب عملاق على مستوى العالم.

يمتلك الحاسب العملاق الذي صنّع في ورش جامعة امير كبير القدرة على الارتباط بالشبكة الوطنية للحواسب العملاقة في البلاد، ويستطيع التحكم بصورة كلية في مكونات الشبكة الوطنية المادية والبرمجية. ويدعم ارتباط الحواسب

[27] . راجع تفاصيل الموضوع على الموقع:
https://web.archive.org/web/20071220190310/http://www.iran-daily.com/1386/3015/html/index.htm

[28] . راجع الخبر المنشور على الموقع: ***http://www.payvand.com/news/11/feb/1248.html***.

العملاقة بهذه الشبكة، قدرتها على معالجة حزمة من المسائل الهندسية والتقنية المعقدة، من خلال توظيف سلسلة من علميات الحوسبة المعقدة والذكية (*Khaksar&Khaksar,2015*).

4 . 3 . تطوير قدرات الحروب الالكترونية ومعدات أمن المعلومات:

ولتطوير منظوماتها الدفاعية، وترسيخ قدراتها العسكرية التي ترجح كفتها في المنطقة، فلم تقتصر إنجازات الكوادر الإيرانية على انتاج الحواسب العملاقة، ومعالجاتها المتطورة، فقد انتجت على المستوى المحلي الكثير من أدوات المعلومات والاتصالات، وبمواصفات تقنية متميزة لخدمة خطط التنمية في قطاع المعلومات والاتصالات الإيراني، سواء كان على صعيد دعم التقنية النووية التي تفتقر الى أدوات معلومات واتصالات، ومسيطرات منطقية قد يحول الحصار المفروض على إيران دون حصولها عليها، ولترسيخ بنية تحتية رصينة للمعلومات والاتصالات تدعم الكثير من مشاريعها الحالية، وخططها المستقبلية غير المعلنة.

4 . 3 . 1 . تطوير قدرات الحرب الالكترونية:

نجحت إيران في تفكيك عناصر الكثير من المنظومات العسكرية للمعسكر الغربي، التي غنمتها من الجيش العراقي خلال الحرب العراقية ـ الإيرانية، وبفضل تعاونها العسكري والتقني مع كوريا الشمالية، فطورت معرفة كوادرها المتخصصة بتقنية التصنيع الحربي ودعمت فرص نجاحهم في تصنيع منظومات رادار متطورة، تعمل ضمن شبكة معلومات متكاملة.

كذلك نجحت بالدخول الى ساحة الحروب الالكترونية، وطوّرت مجموعة متنوعة من التقنيات التي فرضت حضورها في فضاء الحروب السيبرانية وباعتراف الولايات المتحدة، والكثير من الدول الأوربية.

4 . 3 . 2 . تطوير منتجات أمن شبكات المعلومات:

نشب عن غياب الثقة لدى الإدارة الحكومية في إيران، والجهات المهيمنة على صناعة القرارات، والمؤسسات العسكرية والأمنية مثل: الحرس الثوري الإيراني والباسيج بسلامة المنتجات السيبرانية للغرب، والتي تلعب دوراً مهماً في أنشطة الفضاء السيبراني والاتصالات الإيراني، الى التوجّه نحو انتاج الكثير من هذه المعدات بواسطة الكوادر التقنية الوطنية، وبصرف النظر عن الكلف المترتبة عن هذا النمط من الإنتاج لضمان سلامة الجدار الأمني المتين الذي يريدون ترسيخ جذوره حول فضاء النشاط السيبراني الوطني.

فوفرت الحكومة دعماً غير محدود لدعم القطاع الحكومي، وشركات القطاع الخاص لتطوير قدراتهم التقنية وإنتاج معدات وأدوات رقمية تستخدم في قطاع أمن المعلومات والشبكات. وقد نجحت إحدى هذه الشركات بإنتاج منظومة كف رقمية *Filtering System* أطلق عليها *Separ* أدخلت في منظومة شبكات المعلومات الإيرانية، لكف ومنع تسلل المعلومات المناهضة لمنظومة النظام السياسية والعقدية ضمن فضاء الفيض السيبراني بالبلاد (*Khaksar&Khaksar,2015*).

وقد أحرزت هذه الشركات تقدماً ملموساً في هذا المجال من الصناعات، وبدأت بضخ انتاجها من معدات أمن المعلومات والشبكات، وبدأت بتجهيز قطاع الاتصالات والمعلومات الإيراني (العام والخاص) بمنتجاتها مثل: الجدران

النارية، ومرشحات الكفّ السيبراني، والأقراص الآمنة، ومعدات التخويل *Authentication*، والتطبيقات البرمجية التي تقوم بمهمة مراقبة وترشيح محتوى الفيض السيبراني، وإغلاق منافذ الشبكات الافتراضية ـ الخاصة *VPN*.

4 . 4 . البحث والتطوير في قطاع المعلومات والاتصالات:

أنشئ مركز إيران لبحوث الاتصالات *Iran Telecommunications Research Center ITRC* عام 1970 وبالتعاون بين جامعة طهران، والحكومة اليابانية *NTT* لإجراء سلسلة من البحوث المشتركة في قطاع الاتصالات. وبعد أن جاءت الثورة الإسلامية في عقد الثمانينات من القرن العشرين تحول اسم المركز الى *TCI* حيث توسعت دائرة اهتمام المركز على المستوى الوطني في بدايات عام 2005، مع توفير دعم مالي مفتوح من قبل وزارة تقنية المعلومات والاتصالات بعد أن أضحى ارتباط إدارة المركز بالوزارة وفكّ ارتباطه من جامعة طهران.

وقد تعرض المركز الى أكثر من صدمة (خلال السنتين 2006-2007) نشبت عن تذبذب قرار الإدارة الحكومية حول استبقائه في القطاع الحكومي أو الحاقه بالقطاع الخاص، الأمر الذي انعكس بقوة على سياساته البحثية والتطويرية، فتوقفت الكثير من مشاريعه البحثية، واضطرّت إدارته الى تسريح الكثير من كوادره العلمية. أما على صعيد تمويل أنشطته البحثية والتطويرية، فقد اضطر الى الاستعانة بتمويل من مصادر خارجية، لتغطية نفقات أنشطته من المؤسسات التي تروم الحصول على خدماته ومشورته التقنية.

5 . 4 . حاضنات ابتكار وحدائق تقنية:

سعت إيران نحو إنشاء العديد من حاضنات الابتكار *Innovation Incubators* وحدائق التقنية *Technology Parks* لضمان ترجمة الابتكارات والأفكار التقنية الى مشاريع يمكن أن تدعم الاقتصاد الوطني.

ففي عام 2012 توفرت في إيران 31 حديقة علوم وتقنية، استوطنت على عموم رقعة البلاد، لم تلبث ازداد عديدها في عام 2014 الى 930 حديقة ومنطقة صناعية، توفرت 731 منها لأن تترجم الى مشاريع منتجة للقطاع الخاص (*Wikipedia,2015*). وتخطط الحكومة الايرانية لإنشاء 50-60 حديقة تقنية قبل نهاية عام 2015 وكجزء من برنامج التنمية الاجتماع-اقتصادي للبلاد عام 2015.

وقد حاولنا استقصاء أهم الحدائق العلمية والتقنية ذات الصلة بتقنية المعلومات والاتصالات، وتطبيقاتها، فأودعناها في الجدول (1 - 25) والتي تعد بيئة داعمة لمجتمع المعلومات والمعرفة في إيران.

الجدول (1 - 25) ـ أهم حدائق العلوم والتقنية الداعمة لمجتمع المعلومات في إيران.

الحديقة العلمية أو التقنية	مجال النشاط	الموقع
حديقة جولان للعلوم والتقنية.	الالكترونيات، والمعلومات والاتصالات	جولان
حديقة بارديس التقنية.	الالكترونيات، تقنيات المعلومات والاتصالات، التقنيات فائقة الدقة.	طهران
حديقة طهران للبرمجيات وتقنيات المعلومات.	برمجيات الحواسب، وتقنيات المعلومات.	طهران
حديقة جامعة طهران للعلوم والتقنية.	تقنيات هندسية متنوعة.	طهران
حديقة خراسان للعلوم والتقنية.	تقنيات هندسية متقدمة.	خراسان
حديقة شيخ بهائي للتقنية والعلوم.	تقنيات المعلومات والاتصالات.	أصفهان

المصدر: *Wikipedia, 2015*.

وتوفر هذه الحدائق التقنية والعلمية، بالإضافة الى حاضنات الابتكار مناخاً داعماً للابتكارات الشابة في مجال تقنية المعلومات والاتصالات، وهندسة البرمجيات، والحلول الهندسية، والتي تمهد لإنشاء مشاريع محلية ترسّخ جذور مجتمع المعلومات والمعرفة في عموم البلاد.

نجحت الشركات البرمجية التي استوطنت في حدائق تقنيات المعلومات والاتصالات المنتشرة في عموم محافظة طهران، ومراكز بحوث المعلومات في الجامعات الإيرانية بإنتاج منصات وطنية للبريد الالكتروني والرسائل السريعة مثل: *TD Messenger* الذي أنتجته شركة *Tehran Data*، وأكثر من آلة محلية للبحث على مواقع الانترنيت مثل: *Yooz.ir*، و *Gorogr.ir*، ومواقع للتجارة الالكترونية مثل: *Digikala.ir*، وأخرى للتعلم الالكتروني استخدمتها جامعة بيامي نور، وبرامج للتواصل الاجتماعي مثل: *Aparat.ir* (*Wikipedia,2015*).

وقامت كذلك بإنتاج برمجيات مكتبية تحاكي الخدمات التي تقدمها حزمة *Microsoft Office*، وأخرى لإدارة قواعد البيانات، ولإدارة الحسابات والرقابة المالية. كما نجحت جامعة شيراز بإنتاج برنامج حماية أطلق عليه اسم *APA*. أما التطبيقات التي تدعم آلة الإنتاج الصناعي والدفاعي، والنووي فهي كثيرة جداً ولا تكاد تفصح عن هويتها الجهات التي تعمل بجد على إنتاجها وتطوير قدراتها البرمجية من خلال تطبيقات الحوسبة الذكية.

بالمقابل وهناك صناعات برمجية محلية تعتمد على استيراد حزم برمجية (تعدها الشركات البرمجية حسب طلب الشركات البرمجية الإيرانية) من خارج البلاد لغرض إعداد تطبيقات محلية تترجم من خلالها قوائم التطبيقات، وتكيّف إجراءاتها لتلبية الحاجات المحلية. وتشكل هذه البرمجيات المستوردة حوالي 95% من هذا النوع من التطبيقات التي تنتج في البلاد (*EIU,2004*).

وتستقر معظم هذه الشركات في المساحة المخصصة لمشروع حديقة تقنية المعلومات والاتصالات *IT Park* الذي أنشئ في بدايات عام 2004 بمدينة طهران، حيث تتوفر البنية التحتية اللازمة لدعم عمل هذه الشركات. بيد أن التقارير التي عنيت بدراسة هذا القطاع قد أشارت الى غياب التنسيق بين هذه الشركات، حيث تعمل كل شركة بمعزل عن بقية الشركات، الأمر الذي أفقد هذا القطاع القدرة على تكوين لبنة داعمة لصناعة برمجية متكاملة.

5 . المحتوى السيبراني الإيراني:

أطلق اصطلاح المحتوى السيبراني *e-Content* على حصيلة النتاج السيبراني الذي يستودع في مواقع الويب المنتشرة في بيئة شبكة الانترنيت، وشبكات المعلومات المحلية. وتشمل مادة النتاج السيبراني كل من النصوص، والوسائط المتعددة، والتطبيقات السيبرانية بمختلف أشكالها، والخرائط، وجميع اشكال الخطاب الإنساني المرقمن (*ESCWA,2012*).

ويشمل المحتوى السيبراني الايراني جميع النصوص التي أودعت على مواقع الويب المنتشرة بكثافة على شبكة الانترنيت، أو في المستودعات السيبرانية المحلية، سواء كانت مادة هذا المحتوى: نصاً مدوّناً، أم مادة سمعية، أو بصرية، شريطة أن تكون المادة معالجة بالتقنيات السيبرانية، ومفهرسة بأسلوب يسهل التعامل معها(*ITU,2012*).

وقد بذلت إيران جهوداً كبيرة (خلال السنوات الأخيرة) في سعيها الدؤوب الى تطوير المحتوى السيبراني من خلال تبني ودعم مجموعة من المشاريع الوطنية لتوطيد حضور اللغة والثقافة الفارسية في الفضاء السيبراني المحلي، تمهيداً للانفتاح على الفضاء الثقافي التراثي العولمي لإظهار المكانة المتميزة التي تحتلها الحضارة الإيرانية بين بقية الحضارات.

وتعد المكتبات من أولى المناطق التي تلقت عناية لرقمنة محتواها، وربط مستودعاتها بشبكات معلومات محلية. وتعود بدايات إدارة محتوى المكتبات الإيرانية الى برنامج اقترح في عام 1969 وبوشر بمرحلته الريادية *Pilot Phase* في مركز إيران للمعلومات العلمية والتوثيق *IranDoc*. وقد التحقت في عام 1973 حوالي 47 مكتبة وطنية بهذا المشروع، ثم تزايد عديدها الى 141 مكتبة في بدايات عام 1981[29].

وقد أسهم تغلغل تقنيات المعلومات والاتصالات في إيران، مع تزايد حجم المحتوى السيبراني الفارسي في تشجيع أكثر من جهة على المباشرة بمعالجة مادة المحتوى، وتحويلها الى نسق رقمي، مع انتخاب بوابات لعرض المحتوى، وإعداد تطبيقات برمجية، وآلات بحث لتمكين المستخدم الإيراني من بلوغ المادة المعرفية المستوطنة في المحتوى السيبراني.

ولعل من أهم المشاريع التي عنيت برقمنة، ومعالجة، وأرشفة، وعرض المحتوى السيبراني الفارسي خلال السنوات الأخيرة: برامج الجمعية الإيرانية للمحتوى الوطني *ICNC*، والنظام المتكامل لمكتبات جامعة آزاد الإسلامية *SIKA*، والبرنامج التعاوني لمكتبات أستاني قدس رازافي *Thamen*، وبرنامج المكتبات العامة الإيرانية *SAMAN*، وشبكة مكتبة بلدية طهران وبالتعاون مع الجمعية الإيرانية للمحتوى السيبراني (*Ghorbani, et., al.,2015*).

أنشئت الجمعية الإيرانية للمحتوى الوطني عام 2008 وبناء على مقترح تقدم به معهد تبيان *Tebyan* ليمتد نشاطها على عموم الرقعة الجغرافية لإيران، وتنهض بمهمة التنسيق ولم شمل بين الجهات التي تمتلك المحتوى، وتلك التي تقوم بتسليعه وتسويقه رقمياً عبر بوابات شبكات المعلومات المحلية ومواقع فضاء الانترنيت. وتألف الهيكل التنظيمي لأعضاء الجمعية من ممثلي مجموعة من المؤسسات الحكومية (بلغ عدد المكتبات والمراكز الملتحقة في المرحلة الأولى 21 مكتبة ومركز) تم توزيعهم على عدة مراكز، منها المركز الأساسي الذي يعنى بصياغة سياسة المركز وأهدافه على صعيد معالجة المحتوى السيبراني، بينما عنيت بقية المراكز بجمع، ومعالجة، وأرشفة المحتوى وانتقاء الأسلوب المناسب لتوفيره رقمياً للمواطن الإيراني، والمؤسسات العلمية الوطنية، مع التخطيط لفرصة عرض مادة المحتوى على المستوى العولمي (*Ghorbani, et., al.,2015*).

ولعل من أهم أعضاء هذه الجمعية الوطنية، أولئك الذين ينتمون الى: المكتبة الوطنية والأرشيف الإيراني، مكتبة ومتحف ومركز وثائق البرلمان الإيراني، المكتبة المركزية في جامعة طهران، ومؤسسة الموسوعة الإسلامية، والمعهد الإيراني لبحوث السيبرانية وتقنياتها.

وقد رعت هذه الجمعية وأشرفت على مجموعة من مشاريع المحتوى السيبراني الإيراني والتي أسهمت في توفير محتوى رقمي يدعم عملية الارتقاء بثقافة المواطن الإيراني، مع توفير كم ضخم من البيانات والمعلومات التي توزعت بين عدد كبير من مكتبات محلية، وأخرى وطنية ـ أنظر الجدول (1 - 26).

[29] . لم يلبث أن توقف هذا المشروع بعد مدة قصيرة بسبب مشاكل تقنية وأخرى تمويلية، ثم عاد ببداية جديدة في عام 1991.

الجدول (1 - 26) ـ أهم مشاريع المحتوى السيبراني التي ولدت في رحاب الجمعية الإيرانية للمحتوى الوطني.

المشروع	التفاصيل
النظام المتكامل لمكتبات جامعة آزاد *SIKA*.	نسقت إدارة جامعة آزاد مع شركة *Nosa* الإيرانية لربط نظام *SIKA* المتكامل بواسطة تطبيق برمجي محلي، والذي أتاح لجميع الجامعات الإيرانية فرصة البحث في مادة المحتوى المتوفر في هذه الجامعة، مع بدايات عام 2011.
البرنامج التعاوني لمكتبات أستاني قدس رازافي.	بوشر بمشروع *Thamen* لتلبية احتياجات هذا المشروع، والتي تضمنت معالجة محتوى مؤسسة المكتبات والمتاحف والوثائق لعقدين من الزمن. واستهدف المشروع رقمنة المحتوى وتوفير فرصة نشره عبر شبكات المعلومات المحلية ومواقع الانترنيت للارتقاء بثقافة المواطن الإيراني، وتسهيل الوصول الى المكتبات الضخمة الموجودة في مدينة مشهد (بلغ عدد مستخدمي المشروع 1.7 مليون مستخدم، وفر لهم 600,000 مورد رقمي للمعلومات).
برنامج المكتبات العامة الإيرانية *SAMAN*.	يوفر برنامج *SAMAN* فرصة تكامل جميع المكتبات العامة الإيرانية في مكتبة واحدة توفر لمستخدميها فرصة الوصول الى محتوى جميعها هذه المكتبات (يبلغ عددها 2075 مكتبة) من خلال بوابة رقمية موحدة. وقد صممت الكوادر السيبرانية الإيرانية بيئة برمجية متكاملة لإدارة المحتوى وتوفير فرصة الوصول الى المفردة المعرفية المطلوبة، مع إمكانية الإجابة على استفسارات المستخدم واقتراح حلول ذكية لبلوغ ما يريده.
شبكة مكتبة فنون طهران المحلية ومؤسستها الثقافية.	توفر هذه الشبكة لمستخدميها فرصة الوصول الى أكثر من 1.4 مليون كتاب، و2 مليون مقال تتوفر في 80 مكتبة محلية تتوزع في أماكن مختلفة من مدينة طهران. ويوفر نظام *Thana* فرصة استخدام شبكات التواصل الاجتماعي للنقاش حول مادة المحتوى مع وجود نظام مراقبة لهذه الشبكات التواصلية. ويوفر النظام حزمة داعمة لعمليات البحث مع قواميس لغوية وقاموس مرادفات تساعد المستخدم على توسيع دائرة بحثه عن مادة المحتوى السيبراني المطلوب.
مشروع المكتبة المحلية لمدينة أصفهان.	بوشر بالمشروع منذ عام 2006 وبمساهمة مكتبة بلدية أصفهان ومشاركة 9 مكتبات من مكتبات المدينة. وقد وفر المشروع للمستخدمين فرصة المشاركة بالمحتوى السيبراني لمكتبات: مكتبات بلدية أصفهان، وجامعة أصفهان، جامعة أصفهان للعلوم الطبية، وجامعة أصفهان الصناعية، وغيرها من المكتبات السيبرانية المتوفرة في المدينة. وقد استخدم نظام *Thana* لدعم المستخدمين وضمان بلوغهم للمادة المعرفية التي يريدونها.

المصدر: أعدت مادة الجدول من *Ghorbani, et., al.,2015*.

ويضاف الى النشاط الذي تمارسه الجمعية، النشاط المتميز لمؤسسة أرشيف إيران الوطني *NLAI* الإيرانية التي توجه جل عنايتها واهتمامها بالحفاظ على الأرشيف الحكومي، الوطني والتاريخي، ورقمنته لتحقيق مهمة الحفاظ عليه من التلف، وتوفير بيئة رقمية مناسبة لنشره وتداوله داخل حدود إيران وعلى المستوى العولمي.

ولضمان تحقيق أهدافها فقد عمدت هذه المؤسسة الى التنسيق مع جهات متعددة في البلاد لتطوير تطبيقات برمجية، ومعدات شبكاتية وحواسب لدعم تشغيله، مع تحديد أولويات عمليات رقمنة المحتوى، ومعالجته، مع تبني معايير سليمة للحفاظ على مادة المحتوى، في مستودعات رقمية، ومراكز للبيانات، في ظل سياسة واضحة ورشيدة لضمان أمنه وسلامته بوصفه تراثاً قومياً للبلاد وتعبيراً عن هويتها الأصيلة (*Samiee&Davallu,2014*).

من جهة أخرى، بدأ المحتوى السيبراني الإيراني بالتسلل تدريجياً الى فضاء الانترنيت العولمي، ورغم الرقابة المشددة التي مارسها النظام الإيراني، على أنشطة إنشاء المحتوى وتطويره في الفضاء الجديد. ويمكن ملاحظة بعض جوانب هذا الحضور من خلال نتائج الدراسة التي قامت بها

مجموعة من الباحثين الإيرانيين للتنقيب عن حضور المحتوى السيبراني الإيراني ضمن آلتي البحث الشهيرتين *Google*، و*Yahoo* ومن خلال تتبع الملفات التي استودعت ضمن نطاق المستوى الأعلى *Top Domain Level* لإيران *.ir* والذي تعدّ مادة خطابه باللغة الفارسية لتتبع مسارات حضور الفكر الإيراني في فضاء الانترنيت (*Shadanpour, et.,al.,2012*).

وقد حاولنا استخلاص لباب ما توصل اليه الباحثين واودعناه في الجدولين (27-28).

الجدول (1 - 27) ـ عدد صفحات الويب الناطقة باللغة الإيرانية والتي بوّبت محتوياتها بمحركي البحث *Google* + *Yahoo*.

اسم النطاق	الصفحات المبوبة على محرك البحث	
Domain Name	***Google***	***Yahoo***
.ir/	23,300,000	23,103,052
.ac.ir/	1,470,000	1,590,075
.org.ir	140,000	168,012
.gov.ir/	2,840,000	378,003
.co.ir	73,100	109,000
.sch.ir	11,500	18,300
.id.ir	1,600	13,900
.net.ir	1,280	1,510
المجموع	27,837,480	27,181417

المصدر: *Shadanpour, et.,al.,2012*.

الجدول (1 - 28) ـ أهم أنواع الملفات التي استودع فيها المحتوى السيبراني الإيراني على الانترنيت.

نوع الملف	النطاق السيبراني الذي تستودع فيه مادة المحتوى السيبراني							
	.ir/	/id.ir	/sch.ir	/net.ir	/gov.ir	/org.ir	/co.ir	/ac.ir
HTM	1,040,000	99	760	42	13,200	3,160	4,560	60,300
HTML	2,450,000	1,240	196	787	56,200	10,900	17,800	136,000
ASPX	11,200,000	24	4,190	314	627,000	18,600	9,190	310,000
PHP	3,840,000	1,080	3,180	71	66,200	66,100	12,400	487,000
PDF	187,000	6	240	75	4,850	4,760	3,380	110,000
ASP	2,900,000	0	974	117	10,500	10,600	1,720	132,000
SWF	19,600	9	1,260	7	107	104	443	1,870
DOC	17,100	4	455	115	469	460	458	17,400
PPT	2,640	0	3	6	133	131	138	4,710
XLS	1,920	0	3	4	442	402	105	1,360
XML	43,400	0	26	1	152	152	65	365
TXT	32,600	0	2	0	12,200	14,000	34	387

المصدر: *Shadanpour, et.,al.,2012*.

ورغم إقرار أعضاء هذه المجموعة بعجزهم عن العثور على جميع تفاصيل حضور المحتوى السيبراني في مستودعات هذين المحركين، إلا أننا يمكننا القول أن إصرار الإيرانيين على إثبات هويتهم، وتوطيد حضورها في فضاء الانترنيت العولمي، قد نجح في إنتاج محتوى رقمي يعكس جزءاً من بصمة الحضور القومي للبلاد في هذا البلاد.

وأسهمت التحولات في التوجهات السياسية بالبلاد الى توجيه الحكومة المزيد من عنايتها الى مشاريع جديدة لتطوير المحتوى السيبراني الإيراني خلال السنوات الخمس الأخيرة ـ أنظر الجدول (1 - 29).

الجدول (1 - 29) ـ من مشاريع رعاية وتطوير المحتوى السيبراني الإيراني على الانترنيت.

المشروع	التفاصيل
مشروع تبيان *Tebyan*.	بوابة الكترونية أنشأتها مؤسسة التنمية الإسلامية تضم أكثر من 35 GB من البيانات السيبرانية حول المحتوى الإسلامي والثقافي الموجه الى الشباب الإيراني. يمتلك الموقع 30 مجهز لخدمة الانترنيت، ويزوره أكثر من 300 ألف زائر يومياً.
مشروع *TASMA*.	أنشئ بواسطة مؤسسة *HCID* في عام 2006 لتشجيع وتطوير المحتوى السيبراني الناطق باللغة الإيرانية.

المصدر: *Tabesh, et., al.,2004/ Davarinejad&Saffari,2011* .

وتمر عملية إنتاج المحتوى السيبراني هذه الأيام، في إيران، بقفزات متسارعة لتعويض التباطؤ الذي ساد هذا النشاط قبل أكثر من عقد من الزمان. فلم نعد نعثر على صحيفة، او شركة من شركات القطاع لا تمتلك موقعاً مستقلاً في فضاء الويب، أما المؤسسات الحكومية فقد وطدت حضورها، وحرصت على عرض أنشطتها في مواقع لم تعد محصورة في النطق باللغة الفارسية، بعد أن أدرجت اللغات الإنجليزية والالمانية والفرنسية في قوائمها لبيان مستوى التطور الذي بلغته البلاد في فضاء يقيم فيه مواطنون من كل بلاد كرتنا الأرضية.

ويلاحظ عدم اهتمام الإدارة الحكومية إلا باللغة الفارسية في صناعة مادة خطابها السيبراني، مع إغفال بقية اللغات التي تنطق بها الأقليات الموجودة في البلاد، مثل: الأزيرية، والكردية، والأرمينية، وغيرها من اللغات أو اللهجات.

وقد اجملت الدراسة التي قامت بها مجموعة من الباحثين الإيرانيين، أهم الجهات التي تقوم بإنتاج المحتوى السيبراني في إيران كما يأتي (*Tabesh, et., al.,2004*):

1 . وكالات الإعلام:

تعد وكالة أخبار الحكومة الإسلامية بإيران *IRNA*، ووكالة البث لجمهورية إيران الإسلامية *IRIB* المؤسستين الرائدتين في إنتاج المحتوى السيبراني على الانترنيت من خلال بثّ اخبار الثورة الإسلامية، والصدع بإنجازاتها لعموم العالم الإسلامي، ودول العالم المختلفة.

وتقوم بالوقت ذاته، مؤسسات النشر والطباعة الإيرانية بإصدار نسخ الكترونية من منشوراتها ومطبوعاتها على مواقعها المقيمة في فضاء الانترنيت، وبأكثر من لغة في بعض الأحيان. ولعل من أهم هذه المواقع موقع جريدة *Hamshahri* التي تمتلك أكبر عدد من الزوار في فضاء ايران الإعلامي، ومواقع جرائد ومطبوعات أنشأتها أحزاب تساهم في تشكيل المشهد السياسي بالبلاد.

2 . الخطاب الديني:

تمارس المؤسسة الدينية في إيران دوراً ريادياً في إنتاج ونشر الخطاب الديني ـ الشيعي في عموم العالم الإسلامي، ومن خلال الدور الفاعل الذي تمارسه مرجعياتها في قم وطهران، وغيرها من مراكز توطن الخطاب العقدي والفقهي للمذهب الشيعي. وتتميز مؤسسات هذه المرجعيات بنشاط مميز على صعيد إنتاج ورقمنة خطاب المذهب الشيعي، كما انها تلقى دعماً غير محدود من قبل المجلس الأعلى للثورة، وتموّل من أوقف المؤسسات الدينية.

ويقبل على هذا المحتوى السيبراني عدد كبير جداً من المواطنين الإيرانيين، إضافة الى إقبال أتباع المذهب الشيعي في منطقة الشرق الأوسط، وشرق آسيا، فبرز سوق جيد لترويج المحتوى السيبراني الديني، وبدأت الشركات البرمجية في إيران بصناعة موسوعات وبرمجيات لمعالجة المحتوى السيبراني للخطاب العقدي والفقهي الشيعي.

3 . التعليم:

أسهم الاهتمام الكبير للإدارة الحكومية الإيرانية بتعليم الأطفال والشباب، ودعم التحاقهم بالمعاهد العليا ومؤسسات التعليم الجامعي في بروز سوق واسع هرعت الشركات الصغير والمتوسطة الإيرانية الى المشاركة فيه من خلال تسليع محتوى المواد التعليمية، وإعداد وسائط رقيمة للبرامج التعليمية، والتدريبية لمختلف مراحل التعليم في إيران.

وقد مارست عملية التحوّل نحو التعليم الالكتروني دوراً جوهرياً في بروز صناعة برمجية تعنى بإصدار نسخ رقمية للمواد التعليمية، على التوازي مع الجهود التي تبذلها مؤسسات التربية والتعليم، والتعليم العالي الحكومية.

4 . الثقافة والسياحة:

تعكف اكثر من مؤسسة ووزارة في إيران على إنتاج ونشر المحتوى السيبراني الذي يعالج الثروة الثقافية والتاريخية، التي تمتد لبضعة آلاف من السنين، في عمق الحضور التاريخي للبلاد. ومن هذه المؤسسات يشخص أمامنا معهد علوم إيران *Iranology*، ومؤسسة الارشاد الإسلامية، وبحضور من شركات إيرانية من القطاع الخاص لإنتاج أقراص ليزرية، ومواقع ويب لعرض بعض من ملامح الثقافة الإيرانية العريقة وماضيها التاريخي التليد.

5 . النتاج العلمي والبحثي:

بعد أن سادت حركة عملية ناشطة في عموم المؤسسات البحثية، والتقنية، والأكاديمية في إيران خلال أكثر من عقدين من الزمن، برزت الحاجة الى جمع واستقصاء مادة هذه الأنشطة، وأرشفتها، ومعالجتها، قبل أن تستودع في مستودعات رقمية وطنية، تدار مادتها بواسطة برمجيات ذكية تذلل الطريق امام طلبة العلم، والباحثين في إيران أثناء ممارستهم لمختلف اشكال الأنشطة البحثية.

وقد نهضت وزارة العلوم والبحث والتقنية بمهمة إنجاز هذه المهمة الحيوية، فكلفت مركز المعلومات والوثائق العلمية في إيران بجمع ونشر جميع الوثائق والمعلومات العلمية، في مواقع الويب الخاصة بها. وتكاد تنفرد مؤسسات القطاع الحكومي بهذا النمط من النشاط السيبراني، كما ويلاحظ أن جل هذه المستودعات لا ترتبط بشبكة الانترنيت، ويقتصر ارتباطها على الشبكات الوطنية الإيرانية، حرصاً على الاحتفاظ بسرية النتائج التي بلغتها القطاعات العلمية والتقنية في البلاد بعيدة عن الاختراق الذي يمكن أن يمارس على محتويات مواقع الويب.

بصورة عامة، يمكننا القول أن المحتوى السيبراني الإيراني لا زال في مرحلة البدايات، كما أن انحباسه في دائرة اللسان الفارسي قد قلل من مستويات حضوره العولمي في فضاء الانترنيت، فبقي موقوفاً امام غير الناطقين بهذه اللغة.

وقد حاولنا تقييم بعض مواقع المحتوى السيبراني الإيراني بواسطة معايير تقييم صفحات الويب *ALEXA* وانتخبنا هذه المواقع بحيث تشمل معظم فئات إنتاج المحتوى السيبراني هذه الأيام ـ أنظر الجدول (1 - 30).

الجدول (1 - 30) ـ نتائج تقييم صفحات ويب مواقع منتخبة للمحتوى السيبراني الإيراني المعروض على الانترنيت ـ الربع الرابع من عام 2015.

الموقع	الحقل	المرتبة		جغرافية الزوار		توقيتات الزيارة	
		العولمية	الوطنية	إيران	خارجها	تكرار زيارة الصفحة	وقت اللبث دقيقة
Hamshahri.	إعلامي	866,613	30,810	57.1 %	39.6 %	1.0	1:57
Roshid.ir.	تعليمي	13,813	260	88.7 %	3.2 %	1.73	1:58
مكتبة نور السيبرانية.	تعليم عالي	316,468	7,550	98.1 %	...	3.3	3:27
Shia Books.	مكتبة دينية	1,343,246	66,773	100 %	...	15.0	7:17
Sanary	علمية	....	....	....	...	...	...
متحف طهران.	تراث	1,867,904	35,403	87.1 %	...	2.1	2:17

المصدر: استخدام موقع alexa.com.

ويبدو واضحاً أن مواقع المحتوى السيبراني الإيراني، لا زالت متراجعة على صعيد الحضور العولمي بسبب عرض جزء كبير من محتوياتها باللغة الفارسية، أما على الصعيد المحلي فإن المحتوى التعليمي هو الأكثر زيارة بين هذه المواقع بسبب الاقبال المحموم على العملية التعليمية بإيران، (احتل الموقع المرتبة 260).

وتأتي بعدها المواقع الدينية، التي تعرض نسخاً مصورة من خزانة التراث الفقهي والثقافي الشيعي، والتي بلغ نسبة زائريها 100% من داخل حدود إيران، وبمتوسط 15 زيارة للصفحة الواحدة يومياً، وبوقت زيارة يمتد ليصل الى أكثر من سبعة دقائق.

أما مواقع التراث، كالمتاحف، فنلاحظ ان المتحف الوطني الإيراني، لم يفلح بالحصول على مرتبة عولمية مقبولة، ولم يزره سوى مواطنين من داخل حدود إيران، ولم يتجاوز وقت الزيارة الدقيقتين.

6 . مستويات نضج مجتمع المعلومات الإيراني وفق المعايير والمؤشرات الدولية:

أضحت مسألة تحديد انتماء مجتمع من المجتمعات بدائرة مجتمع المعلومات والمعرفة العولمي مرتهنة بما تنطق به مجموعة من المؤشرات والمعايير التي اعتمدتها المؤسسات الدولية لتأييد الانتماء من عدمه، وتحديد مستوى النضوج الذي بلغه المجتمع على صعيد الإيفاء بالتزاماته تجاه الهيكلة المجتمعاتية الجديدة.

وقد انبرت هيئات دولية، مثل الاتحاد الدولي للاتصالات *ITU*، وهيئات ملتحقة بمنظمة الأمم المتحدة، والمنتدى الاقتصادي العالمي *World Economic Forum*، ووحدة الاقتصاد الذكية *EIU* وعكفت على انتخاب مؤشرات، وصياغة معايير لوصف مستويات انتماء المجتمعات الى خطاطة مجتمع المعلومات والمعرفة المعاصر، وبادرت بإجراء

مسوحات ميدانية لكثير من بلدان العالم، واودعت نتائجها في تقارير سنوية تناقش هذه المسألة، وتحدد تراتبية دول العالم على السلّم الذي يصف مستويات الانتماء ونسبة انتشار صبغة المجتمع الجديد في هيكلته المجتمعاتية.

ويلاحظ أن هناك الكثير من الدول قد غاب حضورها عن معيار إحدى الهيئات، أو جميعها، نتيجة لتعثّر عملية الالتحاق، أو وجود بون شاسع بين واقع مجتمعاتها والمواقع الذي تنشد المعايير والمؤشرات توفره لكي تلحق مجتمعها بزمرة المجتمعات الجديدة. بيد أن المراجعة المتأنية قد اثبتت لنا أن إيران هي من إحدى دول المنطقة التي لا نكاد نفتقد حضورها في التراتبية العولمية لتقارير إثبات وجود صبغة المعلومات والمعرفة في مجتمعها المعاصر، مع غياب سمة الانتماء الحميم، شان مجتمعات الكثير من دول الخليج العربي، التي تفوقت على بقية دول المنطقة، ونجحت في أحيان كثيرة في اجتياز دول متقدمة مثل: فرنسا، وألمانيا، واسبانيا، وروسيا، والصين على صعيد تلبية متطلبات الانتماء الى مجتمع المعلومات المعاصر.

ويمكن الوقوف على مستوى نضوج مجتمع المعلومات الإيراني وتحديد المستوى الذي بلغه على تراتبية السلّم العولمي من خلال مراجعة الجدول (1 - 31).

الجدول (1 - 31) ـ مؤشرات النمو في قطاع المعلومات والاتصالات بإيران وفق المعايير العالمية ـ عام 2015.

مؤشر التقييم الدولي	الجهة	مؤشر المرتبة الأولى	المتوسط العولمي	مؤشر إيران	مرتبة إيران
مؤشر نمو أدوات المعلومات والاتصالات *IDI*.	*ITU*	8.86	4.77	4.29	94
مؤشر تطور الحكومة الالكترونية *EGDI*.	*UN*	0.9642	0.4712	0.4508	105
مؤشر الجاهزية الشبكاتية *NRI*.	*World Economic Forum*	6	4.07	3.06	96
مؤشر أمن المعلومات العولمي *GCI*.	*ABI Research*	0.824	0.284	0.294	19
مؤشر التنافسية العولمي.	*World Economic Forum*	5.70	4.21	4.03	83
مؤشر سلة أدوات المعلومات والاتصالات *IPB*.	*ITU*	0.2	9.04	0.6	12

المصدر: *I.I.S.,2015*.

ويبدو جلياً من هذه البيانات أن ايران لم تنجح في الظفر بمرتبة متقدمة تؤشر نحو مستوى نضوج مقبول، وانتماء جيد لحضيرة مجتمعات المعلومات والمعرفة المعاصرة، فلا زال نمو أدوات المعلومات والاتصالات لديها متراجعاً عن المتوسط العولمي، وكذلك الحال بالنسبة لمؤشر الحكومة الالكترونية، ومؤشر الجاهزية الشبكاتية، والتنافسية العولمي، وسلة أدوات المعلومات والاتصالات. الأمر الذي يؤكد (بحسب ما تنطق بها بيانات هذه المؤشرات) وجود أكثر من

فجوة مقيمة في النسيج الشبكاتي لهيكلتها المجتمعاتية، وبنيتها الاتصالية، بحيث لا زال امامها الكثير من العمل، لكي تتجاوز المرتبة المتقدمة التي بلغتها دول المنطقة مثل: قطر، والامارات، والبحرين، والسعودية، وعمان، والكويت، والأردن/ وتركيا.

لقد أثبتت التقارير التي أعدت في أروقة مراكز البحوث الدولية أن ايران لم تفلح بالتفوق على دول بالمنطقة سوى الدول غير النفطية (مثل مصر، ولبنان)، وتلك التي تعصف بها عواصف الربيع العربي، أو الفوضى السياسية والحروب الداخلية (مثل: العراق، وسوريا، واليمن، والسودان).

7 . مراجعة ختامية لمستوى انتماء إيران لمجتمعات المعلومات العولمية:

لقد أثبتت لنا دراسة مختلف عناصر مجتمع المعلومات الإيراني وجود ظاهرة فصام وتناقض بيّن بين مجتمع المعلومات الإيراني بوصفه مظهراً شاملاً لوصف تركيبة مجتمع برمته، يتكامل في ساحتها حضور جميع مؤسساته على التوازي مع حضور دور المواطن الإيراني الذي يستوطن فضاءه، من جهة، وبين البؤر السيبرانية التي نجحت الإدارة الحكومية، وبالتنسيق مع كوادرها العلمية، في استيلادها وحضانتها، بحيث شكّلت هذه البؤر حضوراً منافساً لدول سبقت إيران على صعيد الجاهزية الالكترونية، وجاهزية مجتمعها الشبكاتي، وغيرها من المعايير والمؤشرات التي باتت تحدد مستوى انتماء المجتمع الإيراني الى مجتمع المعلومات المعاصر.

فإذا نظرنا على سبيل المثال الى المشهد العولمي الذي تقيم فيه بيئة البحث وتطبيقات التقانة العالية، في إيران، بالمقارنة مع بقية دول المنطقة ـ أنظر الجدول (1 - 32).

الجدول (1 - 32) ـ خصائص بيئة التعليم والبحث العلمي والتقانة العالية في إيران بالمقارنة مع دول المنطقة عام 2015.

البلد	جودة النظم التعليمية	سمات بيئة البحث وتطبيقات التقانة العالية				
		جودة مراكز البحث والتطوير	وفرة أدوات البحث بالبلاد	دور التقانات المتقدمة بالإنتاج	تعاون الجامعات مع الصناعة في البحث	وفرة العلماء والمهندسين
إسرائيل.	3.7	6.3	4.6	5.3	5.5	5.2
قطر.	5.8	5.4	5.3	5.4	5.4	5.6
السعودية.	4.1	4.2	4.1	4.7	4.2	4.4
الامارات.	5.3	4.8	5.4	5.1	4.7	5.2
البحرين.	4.3	3.2	4.5	4.3	3.3	4.2
الكويت.	3.1	3.2	3.6	3.5	3.1	4.0
عمان.	3.5	3.4	3.8	4.3	3.6	3.7
لبنان.	4.6	2.6	4.2	3.6	2.9	4.6
تركيا.	3.4	3.9	4.4	4.5	3.7	4.2

إيران.	3.0	4.1	3.9	3.6	3.2	4.4
الأردن.	4.6	3.9	4.6	4.3	3.8	5.0
مصر.	2.2	2.4	3.2	3.1	2.4	4.4
سوريا.	…	…	…	…	…	…
العراق.	…	…	…	…	…	…
اليمن.	1.9	1.7	2.9	2.9	2.0	3.1

المصدر: Schwab,et.,al.,2015.

ويلاحظ أن هذه المعايير تشير الى أن إيران متراجعة بشكل كبير، وفق خطاطة المبادئ الدولية، إزاء بقية الدول، ولا تكاد تنافس إلا الأردن، ومصر، وسوريا، والعراق، واليمن.

ولا يخفى سبب تراجع هذه الدول عن المرتبة التي تحتلها إيران، بسبب شحة الموارد (مصر والأردن)، والنزاعات المحلية التي أنهكت كل من: سوريا، والعراق، واليمن.

أما مراجعتنا للمشهد السيبراني، بدءاً بالبنية التحتية للمعلومات والاتصالات، وانتهاء بمؤشرات اقتصاد المعرفة، فيتكرر امامنا المشهد ذاته، وتكاد تتطابق المرتبة المتراجعة التي تحتلها إيران بالمقارنة مع بقية دول المنطقة.

بيد أن كل هذه المعايير والمؤشرات لا تكاد توفر تبريراً للتقدم التقني والسيبراني الذي حققته بالمقارنة مع بقية دول المنطقة، وتفوقها المميز في أكثر من قطاع يكاد يبرهن على تهافت على القيمة الموضوعية التي تتسم بها هذه المعايير في تقييمها لانتماء مجتمع من المجتمعات الى مجتمع المعلومات العولمي، أو غيابه عنه.

ونعود ثانية الى ما أشرنا إليه في فقرة سابقة، وهو أن إيران لم تنجح في استكمال متطلبات الانتماء الى مجتمع المعلومات بجميع مفاصل تركيبتها المجتمعاتية. بيد أنها قد نجحت في تنشيط مجموعة من البؤر التقنية، والسيبرانية، ورعت مجموعة من الكوادر المعرفية بحيث نجحت في تحقيق تفوّق لافت على صعيد منطقة الشرق الأوسط، رغم تكاثر الفجوات في نسيجها الشبكاتي، والتقني، والمعرفي، بحيث وفرت لنفسها فرصة الظفر بمكانة استراتيجية جعلتها تعرض عن هذه المؤشرات وما تتناقلها تقارير المنظمات الدولية التي لا زالت تصرّ على صحة وموضوعية معاييرها في وصف انتماء المجتمعات الى جادة مجتمع المعلومات والمعرفة العولمي، بينما يصدع الواقع الملموس بتهافتها، وتهافت القرارات التي نصنع من خلالها التقييم الاستراتيجي للتعامل مع هذه الدولة أو تلك، أو نقارن (على أساسها) بين مستويات رجحان كفة موازين القوى في منطقة الشرق الأوسط.

الفصل الثاني:
الحضور السيبراني الإيراني في الفضاء السيبراني المكبّل

الفصل الثاني: الحضور السيبراني الإيراني في الفضاء السيبراني المكبّل

1 . تحليل حفريات الانترنيت في إيران:

تعود الحفريات البدائية التي التصقت بها صبغة الانترنيت في تربة فضاء الاتصال الإيراني الى عقد التسعينات من القرن العشرين، والتي بدأت تباشيرها عند المشهد الأخير من حرب الثماني سنوات مع العراق، والتي لم تثني ضراوتها المجتمع الأكاديمي الإيراني، وقلة الخبراء الذين لم يغادروا البلاد بعد الثورة الإسلامية، عن السعي الى توطين التقنية الجديدة، وترسيخ بصماتها في البلاد.

1 . 1 . حفريات الانترنيت في القطاع الأكاديمي الإيراني:

أظهرت تحرياتنا في حفريات الانترنيت بتربة إيران السيبرانية، وجود أحافير تشير الى أن هذه البلاد قد خططت، وسعت للحصول على منفذ للاتصال بالمشروع الأم *ARPANET* الذي نشأت في رحمه شبكة الانترنيت الحالية.

ويعود تاريخ هذه المحاولة الى عام 1987 وبعد أن قامت وكالة مشاريع الدفاع المتطورة *DARPA* بربط عدد من المؤسسات الأكاديمية ومراكز بحوث وزارة الدفاع الأمريكية بخدمات رقمية، شجعت شركة *IBM* على إنشاء شبكة أطلق عليها اسم شبكة *BITNET* امتدت أطرافها الى مجموعة من الجامعات ومراكز البحث الأوربية باتت تعرف بشبكة البحوث الأكاديمية الأوربية *EARN*. لقد نجح معهد *IPM* بالارتباط مع شبكة *BITNET*، ثم قام بعد حين (في بداية عام 1992) بالانضمام الى الشبكة الاوربية *EARN* (*ORN,1999*).

وأسهمت جهود الدكتور محمد جواد لاريجاني بحصول إيران على خط من إدارة جامعة فيينا ضم حوالي 500 عنوان *IP Addresses* مع قبول حضورها ضمن عقدة معلوماتية بالمستوى C (*ORN,1999*).

فانصبغت الانترنيت في بداياتها (في إيران) بصبغة أكاديمية عندما وضع الدكتور لاريجاني (رئيس معهد الدراسات في الفيزياء النظرية والرياضيات *IPM*) اللبنة الأولى لحضور الانترنيت بالبلاد فجعل من الشبكة الأكاديمية والبحثية في المعهد البوابة والمدخل للارتباط الدولي بشبكة الانترنيت. ثم نجح المعهد في القيام بمهمة إدارة أسماء النطاق العلوي للبلاد *TLD* (*www.nic.ir*) (*MOSAIC, 1999*).

وقد توفرت الفرصة، في البداية، أمام ثمانية عشر جامعة ومركز بحث في البلاد للإبحار بفضاء الانترنيت من خلال الاتصال المباشر بشبكة *IPM* (*Rahimi,2003*).

أما بقية الجامعات والمؤسسات العلمية فقد اضطرت الى الوصول للشبكة بواسطة الخط الهاتفي الذي اتسم ببطء الخدمة السيبرانية التي وفّرها لمستخدميه. وبالوقت ذاته فإن غياب شبكات المعلومات المحلية *Local Area Network* عن الكثير من المؤسسات الأكاديمية والبحثية، والمؤسسات الحكومية، في عقد التسعينات، قد أسهم في حصر منافذ وبوابات الخدمة على الإدارات العليا، ومراكز الدراسات العليا، وعبر حاسب منفرد، أو شبكة معلومات ضيّقة (*ICRTC,2005*).

ولم يقتصر الأمر على محدودية المنافذ، وإنما شمل محدودية سرعة الخدمة التي لم تتجاوز سرعة فيضها (في ذلك الوقت) على 9.6 Kbps بسبب تدهور البنية التحتية، ولم يظفر بسرعة 64 Kbps سوى مجموعة محدودة من العاملين على شبكة الانترنيت الرابطة بين بنايات مركز *IPM*، وجامعة جيلان التي تقع في الشمال الغربي من مدينة طهران.

بيد أن حرص المؤسسة الأكاديمية الإيرانية على الالتحاق بفضاء الانترنيت، واستثمار الموارد المعرفية المقيمة في فضائه السيبراني، قد دفعها (في عام 1994) الى إنشاء ثاني أكبر شبكة محلية *Intranet* في الشرق الأوسط (بعد إسرائيل التي

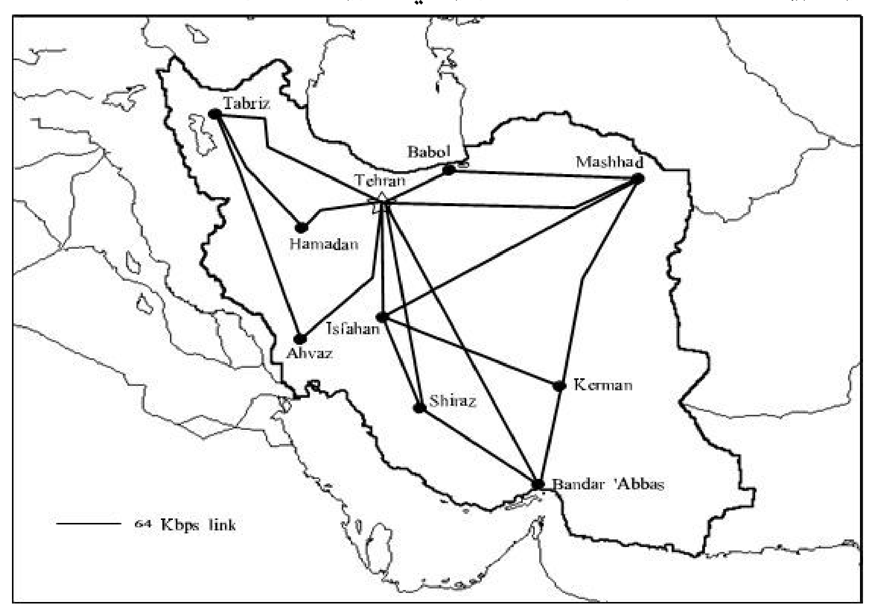
امتلكت أكبر شبكة محلية) وفرت للمستخدمين الإيرانيين فضاءً رقمياً قادر على تلبية حضور طيف واسع من المستخدمين في بيئة الانترنيت تراوحت أعدادهم بين 30,000 الى 60,000 مستخدم (*MOSAIC, 1999*).

1 . 2 . حفريات الانترنيت لدى المؤسسة الحكومية الايرانية:

في مطلع عام 1995 تقدمت شركة اتصالات إيران *TCI* بالتماس الى البرلمان للموافقة على إنشاء شركة عامة، أطلق عليها شركة اتصالات البيانات الإيرانية *DCI* لتكون مسؤولة عن تطوير خدمات تداول البيانات في عموم إيران على أن تهيمن الحكومة على نشاطات هذه الشركة عوضاً عن مجموعة شركات القطاع الخاص[30] *IranPac* التي نهضت بمهمة إدارة وتوزيع البيانات الواردة من خارج البلاد. وقد صودق على إنشاء الشركة في شهر سبتمبر من العام ذاته، وبدأت بالتنسيق مع شركة *TCI* في تنظيم وإدارة سوق خدمات البيانات، مع توجيه عناية خاصة الى خدمة الانترنيت (*MOSAIC, 1999*).

وقد باشرت شركة إيران لتناقل البيانات *DCI* بالمرحلة الأولى من مشروع الانترنيت من خلال توفير متطلبات تزويد 20,000 مستخدم، ثم أنجزت المرحلة الثانية التي وفرت البنية التحتية المطلوبة لتزويد 300,000 اشتراك بخدمة الانترنيت في عموم البلاد.

استمدت الشركة فيضها السيبراني عبر الارتباط بخدمة شبكة الأقمار الصناعية في كندا، ووفرت خدمة الانترنيت بواسطة شبكة امتدت بين عشرة مدن إيرانية في عام 1997، وبحزمة بلغت سرعة فيضها السيبراني *64 Kbps*. بعدئذ هرعت الشركة ذاتها الى ابرام عقد خدمة مع وزارة الاتصال الكويتية، وشركة *Hughes Network Systems* الأمريكية لتأجير خط لخدمة الانترنيت بين العاصمة طهران ونقطة التزويد في الكويت ـ أنظر الشكل (2 - 1).



الشكل (2 - 1) ـ العمود الفقاري لشبكة خدمة الانترنيت التي هيمنت عليها شركة *DCI* في عام 1999 ـ المصدر: (*MOSAIC, 1999*).

ورغم إعلان شركة *DCI* (في بداية عام 1999) عن توفر خدمة الانترنيت لديها وبسرعة ناهزت *2 Mbps* إلا أن ارتفاع كلفة هذه الحزمة السيبرانية حال دون استثمار خدماتها الا من قبل مؤسسات حكومية محدودة بينما رضي جل المشتركين بخدمات الشركة وبحزمتها ذات السرعة البطيئة بسبب الارتفاع في كلف الاشتراك بها (*MOSAIC, 1999*).

30 . تألفت مجموعة الشركات من: شركة *Pars Supaleh*، وشبكة معهد دراسات الفيزياء النظرية والرياضيات، ومركز البيانات الإيرانية . الخارجية.

1 . 3. حفريات الانترنيت لدى القطاع الخاص:

لم تتوفر لدى المؤسسة الحكومة الإيرانية فرصة لدعم دخول القطاع الخاص الإيراني في بيئة اقتصاد الانترنيت، فبقيت شركتي *TCI & DCI* تهيمن على سوق الخدمات السيبرانية، بيد أن هذه الهيمنة المطلقة قد أورثت سوق المعلومات الإيراني سمة غياب التنافس وتراجع مستويات الخدمة التي قدمتها الشركتان للقطاع الخاص.

واتخذ القطاع الخاص الخطوة المهمة الأولى، على صعيد فتح أبواب فضاء الإنترنيت أمام المواطنين الإيرانيين، عندما قامت شركة *N.J.Rad*، إحدى فروع شركة *Pilot Iran*، بإنشاء شبكة معلومات واتصالات إيران *IRANET* في عام 1993. وباشرت هذه الشركة السيبرانية بتزويد المشتركين بها بخدمات متنوعة شملت: الوصول الى مواقع الانترنيت، وخدمات البريد الالكتروني، وتصميم وإنشاء مواقع الويب للأفراد والشركات (*Rahimi,2003*).

ومع بدايات عام 1997 اتجهت شبكة *IRANET* للتعاون مع القطاع الأكاديمي، بوصفه الحاضنة الأولى لخدمة الانترنيت في البلاد، فولّدت مناخاً مناسباً لاستنبات المزيد من شركات تقنيات المعلومات والاتصالات في البلاد، فتزايدت فرص العمل للكوادر السيبرانية، وانتعش الاستثمار في قطاع المعلومات في العاصمة طهران، ومدن أخرى في إيران.

فنشب عن النمو المتسارع في اقتصاد المعلومات بإيران تزايد التحديات التي واجهتها شركة *TCI* التي لم تمتلك القدرة على التكيّف مع حاجات السوق المتنامية بسبب ارتباطها بالهيكلة البيروقراطية لوزارتها، من جهة، وغياب الخبرات لدى كوادرها، من جهة أخرى، فلم تستطع مواكبة النمو السريع في ميدان تقنية المعلومات والاتصالات، واستمرت تلهث للحاق بالقطاع الخاص الذي نال قصب السبق في سوق الخدمات السيبرانية، وتوفير مجهزات الخدمة للمواطنين *ISP*.

وقد انتقلت خدمة الانترنيت نحو المساحة التي يهيمن عليها القطاع التجاري على يد معهد *Neda Rayaneh Institute* (*NRI*)، والذي يعد أول مجهز خدمة تجارية للانترنيت بإيران. وكان المعهد من الشركات غير الربحية التابعة الى حكومة طهران المحلية.

فبدأت الشركة في تجهيز خدمة الانترنيت في الربع الأول من عام 1995، وعبر خطين مستأجرين (سعة كل منهما 9.6 Kbps)، ارتبط أحدهما بشبكة معهد *IPM* المحلية، بينما ارتبط الثاني عبر مستقبلات الأقمار الصناعية مع مجهز خدمة من شركة *Cadvision* في كندا.

شملت حزمة الخدمات السيبرانية التي وفرتها شركة *NRI* أخباراً محلية مفصلة، وخدمات معلوماتية متنوعة، وخدمة بريد الكتروني للمشتركين الايرانيين. وقد عكفت بالوقت ذاته على إصدار وتحديث الصفحات الصفراء *Yellow Pages* لمدينة طهران، ودليل هواتف المستخدمين، ومعلومات متنوعة عن المدينة، مع خارطة طهران التفاعلية *Tehran Interactive Map*.

وقامت الشركة، أيضاً، باستضافة الكثير من صفحات الويب المحلية، وباللغتين الفارسية والانجليزية.

وقد هرعت وزارة البريد والتلغراف والهاتف الإيرانية *MPTT* الى قطع خطوط الشركة، التي ناهزت مائتين خطاً، في شهر آب من عام 1995، بحجة الاستخدام غير الأخلاقي لبعض المشتركين بخدماتها السيبرانية، واستغلالها لإقامة علاقات غير مشروعة بين الجنسين. غير أن حقيقة الأمر هو رغبة كل من شركتي *TCI & DCI* بالهيمنة على سوق الاتصالات في البلاد. لم يستمر الانقطاع طويلاً، ونجحت NRI بإعادة خطوطها للعمل بعد أن التزمت بإظهار رسائل تحذيرية لمستخدميها من مغبّة الاستخدام غير الأخلاقي للخدمات السيبرانية التي وفرتها شبكتها السيبرانية.

وقد برزت في الحقبة ذاتها شركة *Pars Supaleh*، التي استأجرت خطاً من هولندا بلغت سرعته 9.6 Kbps، ووفرت للمشتركين بها فرصة الوصول الى قواعد البيانات التجارية، مثل قواعد بيانات *Dow Jones* وغيرها من بيانات الأسواق

التجارية العالمية. ناهز عدد المشتركين بخدمات هذه الشركة 100 مشتركاً من المؤسسات الحكومية، ومراكز البحوث الصناعية والاقتصادية، التي تفتقر الى تحديث بياناتها في هذا المضمار (*MOSAIC, 1999*). ورغم قيام هذه الشركة بتوفير خدمات أخرى مثل خدمات البريد الالكتروني، وخدمات دعم للمستخدمين، إلا أنها قد اضطرت بعد مدة قصيرة الى وقف نشاطها بسبب قلة أعداد المشتركين، وتراجع أرباحها بشكل كبير.

وقد أثمرت تحرياتنا الجيولوجية في المستويات التي بلغتها حفرياتنا عن تشكيل الإطار العام للتحوّلات التي مرّت فيها شبكة الانترنيت في إيران خلال بضعة عقود، ابتدأت مع نهايات القرن العشرين، ولحين اكتمال العقد الأول من الألفية الجديدة. ويمكن تلخيص نتائج تحرياتنا بما يأتي:

- أسهم الدعم الذي أولته الحكومة الإسلامية بإيران للقطاع الأكاديمي وإيمانها بقدرته على إصلاح واقع البلاد ولملمة البلاد بعد حرب ضروس (اورثت البلاد اقتصاداً ضعيفاً، وتدمير كبير في البنى التحتية للبلاد) بدعم طموح المؤسسة الأكاديمية في الالتحاق بالفضاء السيبراني الجديد، فكانت من الدول الرائدة بمنطقة الشرق الأوسط في إدخال الخدمات السيبرانية الى المؤسسات الأكاديمية والبحثية، والتي كانت سبباً لبلوغ الخدمة الى بقية المؤسسات الحكومية قبل أن تنفتح على القطاع العام وتصل الى المواطنين الإيرانيين في عموم البلاد.
- شهد فضاء الانترنيت نمواً غير مسبوق في إيران، فتوسع حجم حزمة الانترنيت الدولية من 28 Mbps في عام 1999 الى 1.5 Gbps في بدايات عام 2005 (*ICRTC,2005*). كما أن أعداد المشتركين بالخدمة قد ارتفع بوتيرة نافس فيها جميع بلدان المنطقة، حيث ازداد عدد المستخدمين من 132,000 مستخدم عام 2000 ليبلغ عام 2002 أكثر من 1,326,000 مستخدم ـ أنظر الجدول (2 - 1).

الجدول (2 - 1) ـ أعداد المشتركين بخدمة الانترنيت في إيران عند بدايات توفر الخدمة في السنوات 1996-2002.

السنة	عدد المستخدمين	نسبة النمو
1996	2,000	...
1999	48,000	2,300 %
2000	132,000	175 %
2001	418,000	216.7 %
2002	1,326,000	217.2 %

المصدر: *Khiabany&Sreberny,2009*.

- أسهمت التجاذبات الداخلية بين شركات المعلومات الإيرانية، مثل: *TCI&DCI* وتنازعها مع القطاع الأكاديمي للانترنيت المتمثل بمعهد *IPM*، والقطاع الخاص الذي قادته الشركات المجهزة للخدمة في توليد مناخ غير مستقر، انسحبت تأثيراته السلبية على وفرة وجودة خدمة الانترنيت في عموم البلاد. يضاف الى ذلك غياب استراتيجية واضحة لتنمية خدمة الانترنيت، والسعي الى نشرها على مساحة واسعة من الرقعة الجغرافية للبلاد، ولعموم شرائح المجتمع بسبب التجاذبات السياسية والعقدية بين المؤسسة الدينية والمؤسسة السياسية حيث غابت الغايات والأهداف وتداخلت لدى هذه الأطراف، فبقيت خطط التنمية للبنى التحتية منهمكة بتوفير خطوط الهواتف، ومد شبكة الألياف البصرية، مع شحة الفيض الساري في هذه الشبكة العملاقة.

- عندما باشر القطاع الخاص عام 2000 بفتح أبواب مقاهي الانترنيت في كثير من المدن الإيرانية، اشتعلت المنافسة بين شركات القطاع وبدأت أسعار الخدمة بالتراجع السريع، وعمدت المقاهي بتقديم حزمة متنوعة من الخدمات لزبائنها، فانعكس هذا النشاط الاقتصادي للقطاع الخاص على أرباح الشركات الحكومية مثل: *TCI* والتي تحملت خسارة سنوية قدرها 32 مليون دولار في عام 2002، بينما بلغت أرباحها عام 1998 حوالي 20 مليون دولار (*Khiabany&Sreberny,2009*).

- لم تخلو ساحة الهيكلة المؤسسية للانترنيت، في إيران، من تنافس وتجاذب بين مراكز القوى الثلاثة التي هيمنت على جل الأنشطة السائدة فيها. فلقد تنافست شركة اتصالات إيران *DCI* مع معهد *IPM*، والمجلس الأعلى للمعلوماتية *HCI* وتدافعت خططها حول مستقبل خدمة الانترنيت في إيران، ومقدار الحزمة المناسبة لتلبية الاحتياجات المحلية، بقطاعيها الحكومي والخاص فتأخر وصول الخدمة السريعة للبلاد. وقد اضيف الى هذا المناخ المشحون، الحصار الأمريكي الذي مورس على البلاد، والذي أسهم في زيادة حجم العقبات المالية والتقنية أمام الحصول على خوادم سريعة، وتوفير معدات اتصالات، ومعدات للمحطات الأرضية، وغيرها من أدوات المعلومات والاتصالات التي تتطلبها عملية توسيع سعة الخدمة (*ORN,1999*).

- كان لولادة المدونات السيبرانية في الفضاء السيبراني الإيراني في بدايات عام 2000 دوراً جوهرياً في زيادة إقبال الشباب الإيراني على مزاولة حرفة التدوين، وتشكيل الملامح المميزة لأشهر فضاءات التدوين السيبراني في عموم الفضاء السيبراني للانترنيت. وقد توسعت دائرة التدوين السيبراني تدريجياً نتيجة لإقبال شريحة واسعة من الشباب المعارضين لنظام الحكم في البلاد، ولوجود أصوات سياسية معارضة باتت تدعو الى إحداث تغييرات حاسمة في البنية السياسية والتقليل من الهيمنة الغاشمة للمؤسسة الدينية.

- وجد الكثير من السياسيين الإيرانيين، وأفراد المرجعيات الدينية، والمراكز الدينية في مدينة قم وغيرها من مراكز الحركة الشيعية بالبلاد، أن الانترنيت بدأت توفر لهم فضاءَ رحباً لإبلاغ أصواتهم، ونشر آرائهم، وتوسيع رقعة الدعوة الى المذهب الاثني عشري، ونشر فكر وقيم الدولة الإسلامية في إيران، وترسيخ جذورها، داخل حدود البلاد وخارجها. فبدأت صناعة المحتوى السيبراني الشيعي وأودعت في فضائه أعداداً كبيرة من خزانات فقه الامامية وعلومهم النقلية والعقلية.

- نشأ عن توسع دائرة الحضور السيبراني للمفردات العقدية في البلاد، وتنامي حضور الخطاب السياسي المعارض، وانشغال طيف واسع من الشعب الإيراني بترسيخ حضورهم السيبراني، والانتباه الى غياب الحدود والقيود التي سادت البلاد عن فضاء التواصل الجديد توجه اهتمام المؤسستين السياسية والدينية نحو وجود أصوات معارضة باتت تتعالى شيئاً فشيئاً وتستمد قوتها من المميزات الفريدة لهذا الفضاء، ولادة تيار معارض لحضور الانترنيت في إيران، فتوجهت الأنظار، في بدايات عام 2003، نحو حجب الكثير من المواقع، وممارسة عمليات الرقابة على المحتوى، وسن التشريعات التي أسهمت في بث المزيد من القيود في فضاء الانترنيت، وكانت بادرة لنمو وترسّخ اكثر نظم المراقبة السيبرانية على محتوى مواقع الانترنيت، وتقطير المادة المطروحة فيها.

- استثمرت شركات القطاع الحكومي هذه الظاهرة لتوسيع دائرة سيطرتها على فضاء الانترنيت من خلال الهيمنة على منافذ خدمة الانترنيت وحصرها بالمنفذ الذي تمتلكه شركة *TCI*، كما ان ممارسات المراقبة

أصبحت جزءَ لا يتجزأ من هويتها، وأصبح القطاع الخاص للمعلومات أسيراً لسياساتها التي استمرت في تغييب سمة التنافس عن سوق المعلومات في إيران، والسعي المحموم نحو الاستمرار ببسط هيمنتها التي استمدتها من عدم توازن سياسة الحكومة، وتناقض مواقف مؤسساتها في التعامل مع مسألة الانترنيت، وتحديد ملامح حضور المواطن الإيراني في فضائه الذي تزايدت أعداد القيود المفروضة عليه، وتوسعت دائرة الأغلال التي خنقت وغيّبت الحضور السيبراني للمواطن الإيراني فيه.

- نشب عن الحصار الذي فرضته الولايات المتحدة على إيران، وعدم تخصيص الحكومة الإيرانية استثمارات كافية لدعم تقنيات الانترنيت، مع انخفاض دخل المواطن الإيراني، تراجع قدرة شريحة واسعة من الطبقة الوسطى للإيرانيين على اقتناء حاسب (بلغت كلفة الحاسب ضعف متوسط الأجر الشهري للمقيمين في المدن وثلاثة أضعافه في المناطق الريفية بإيران)، كذلك فإن كلفة خدمة الانترنيت العالية، وتراجع سرعة الخدمة أسهمت في تثبيط معدلات النمو، وانحسار انتشار الخدمة قبالة التوجه المحموم لدى المواطنين على الحضور السيبراني في فضاء مفتوح.
- رغم الحصار الذي فرض على إيران بسبب الخلاف مع الغرب حول تفاصيل ملفها النووي، فقد استمرت مؤسساتها السيبرانية بترسيخ حضورها السيبراني العولمي. وكان من إنجازاتها استمرار العمل على استكمال شبكاتها المحلية، وبالخصوص خدمة *IPv6* التي بدأت تجهيز حزمة منها لدول الجوار مثل العراق وأفغانستان، واستضافة مضيفات *DNS* مما منحها الفرصة لتجهيز هذه الخدمة الحيوية ضمن الفضاء السيبراني العولمي (*ReneSys,2015*). وقد تمتعت شركة *TCI* بفرصة توطن مضيف أصول أسماء النطاق[31] *Root Name Server* من بين ثلاثة عشر موقعاً استوطنت الفضاء العولمي لشبكة الانترنيت، الأمر الذي سيسهم في دعم انفتاح كبير لشبكة الانترنيت في إيران على الفضاء العولمي على التوازي مع سياسة الرئيس روحاني التي تدعم انفتاح البلاد على فضاء الانترنيت وتقليل قيود المراقبة على المواقع (*ReneSys,2015*).
- بدأت سرعة الانترنيت بالتحسن تدريجياً في عموم العقد السيبرانية المنتشرة على الرقعة الجغرافية للبلاد، فبلغت في بداية عهد الرئيس حسن روحاني 0.64 Mbps لدى مستخدمي الهواتف المحمولة، والحواسب اللوحية، والحواسب المنضدية، وبعد أن قامت أكثر من شركة إيرانية بتوفير خدمات الحزمة العريضة للانترنيت مثل[32]: *AsiaTech Inc., Communications in Iran, Mobin Net, Pars Online*. وتستمر سعة حزمة خدمات الانترنيت بالازدياد تدريجياً، حيث بلغ متوسط سرعة الخدمة عام 2015 حوالي 1.4 Mbps بحسب الاختبار الذي أجري بواسطة الموقع المتخصص بتقييم سرعة الانترنيت في بلدان العالم المختلفة[33].

2 . موقف المؤسسات الإيرانية من الانترنيت:

توطنت العقد السيبرانية لشبكة الانترنيت في إيران منذ بداية عقد التسعينات من القرن العشرين، واستنبتت أولى براعمها في التربة الأكاديمية التي اتسمت بحيادية تعاملها مع الفيض السيبراني وتوظيفه في اكتساب المزيد من المعارف

[31] . مجموعة من المضيفات التي تتوزع على عموم الخارطة الجغرافية العولمية، وتوفر خدمة لقواعد أصول أسماء النطاق *DNS* لشبكة الانترنيت .
https://www.iana.org/domains/root/servers

[32] . الموقع: *http://www.bandwidthplace.com*.

[33] . الموقع: *http://www.testmy.net/download*.

التقنية، ودعم النشاط الأكاديمي والبحثي لكوادرها داخل أروقة المؤسسات الجامعية وفي بعض مراكز البحوث الوطنية.

ثم تناسلت العقد السيبرانية فبلغت مؤسسات الحكومة، ثم انتقلت باتجاه المجتمع الإيراني، الذي تلقفها ووجه إليها عنايته الخاصة لأسباب عدة. ومن هذه الأسباب أنها تقنية فريدة، وفضاء متخيل كثر الحديث عنه، كما انها شكّلت فرصة ثمينة للانطلاق بعيداً عن القيود الصارمة التي فرضتها ثقافة الثورة الإسلامية بإيران، ومنعها لكثير من الأنشطة التي تعوّد الإيرانيون المعارضين على البوح بها، وترسيخ بصمة هويتهم قبالة المدّ الثوري الجديد. ومثّلت بالوقت ذاته مناخاً مناسباً لتحقيق حلم شباب الثورة الإسلامية في تصدير ثورتهم في فضاء تغيب عنه الحدود السياسية والإقليمية، ويبشر بفرصة انتشار المذهب الجعفري على عموم رقعة البسيطة، والذي يعد تمهيداً لمرحلة الظهور التي انتظرتها أجيال متعددة.

هذا التداخل والمزيج المتناقض من أسباب اقبال جميع الكيانات الإيرانية على التعامل مع فضاء الانترنيت، والسعي الى استثماره لتحقيق غايات متعددة، ومتعارضة في كثير من الأحيان بات السمة المميزة لهذا الفضاء الذي سنحاول التنقير في تربة هذا القطاع من قطاعاته المتكاثرة.

2 . 1 . الجمهورية الإسلامية والانترنيت:

بعد أن انتقلت خدمة الانترنيت من داخل الأروقة البحثية والأكاديمية لمعهد إيران *IPM* وجامعة طهران باتجاه أسوار الحكومة الإيرانية، باشرت الحكومة بسلسلة من الإجراءات لاحتواء عملية حضور الخدمة السيبرانية الجديدة في بنيتها المؤسسية. فعاودت الحكومة النظر بهيكلة وزارة البريد والتلغراف والهاتف *MPTT* (والتي نهضت بمهمة تزويد وتنظيم سوق الاتصالات بالبلاد لغاية عام 2003) وروجعت هيكلتها التنظيمية فأصبحت وزارة المعلومات وتقنيات الاتصالات *MICT* التي كلفت بإدارة فضاء الانترنيت والاتصالات بعموم البلاد. والتحقت بها كل من شركة اتصالات إيران *TCI*، ثم وليدتها شركة اتصالات معلومات إيران *DCI* فكفلت الأولى، وبالتنسيق مع الثانية بمهمة إيصال خدمة الانترنيت للمجمعات السكنية، والمؤسسات التجارية، وجلّ عناصر الاتصالات الأرضية والمحمولة في البلاد.

ثم توجهت بعد حين الى جذب خدمة الانترنيت الى وزاراتها، والمؤسسات الملتحقة بها، مع التوجه نحو رقمنة أرشيفها، وبناء المنافذ السيبرانية لتجاوز البيروقراطية المتفشية في الكثير من المؤسسات، ووظفت المزيد من التطبيقات الالكترونية، وبرامج الأرشفة الالكترونية تمهيداً للمباشرة بمشروع الحكومة الالكترونية الذي تكاثرت تطبيقاتها فشملت برامج التعليم الالكتروني، والرعاية الصحية الالكترونية، وحزمة من الخدمات العامة التي وفرتها لأفراد المجتمع الإيراني.

تلقّت الجمهورية الإسلامية في إيران خدمة الانترنيت من خلال المنفذ الأكاديمي الذي كان له قصب السبق في الارتباط مع فضاء الانترنيت في بدايات عقد التسعينات من القرن العشرين. وقد تعاملت مع فيضها السيبراني بنهج عفوي، ولم تخطط للهيمنة على النبضات السيبرانية التي تسري في هذا الفضاء، أو تفرض محددات على عملية الإبحار بين مواقع الويب، أو تداول الرسائل عبر خدمة البريد الالكتروني، كما هو الحال في دول المنطقة مثل السعودية، ودولة الامارات (*Rahimi,2003*).

في البداية تعاملت الحكومة مع فضاء الانترنيت بوصفه أداة رقمية يمكن أن توفر للبلاد أكثر من فرصة سانحة لتحقيق المزيد من التقدم العلمي، وإيجاد منفذ لاقتصاد البلاد الذي كان يعاني من أزمات متلاحقة، جرّتها الحرب مع العراق، وتعثر خططها التنموية، وتفاقم البطالة بالبلاد. لذا انصب هاجسها على توسيع دائرة انتشار خدمة الانترنيت خارج

حدود المؤسسات الأكاديمية والبحثية، باتجاه بقية مفاصل الدولة، ولم تجد حرجاً في توفير الخدمة للمواطن الإيراني لكي يستثمر محتوى الفضاء في تلبية بعض احتياجاته.

وشاركت وزارة المعلومات وتقنية الاتصالات في إنشاء بيئة رقمية لدعم التطبيقات المحلية في فضاء الانترنيت، فقامت شركة *DCI* بإصدار جريدة رقمية يومية في عام 1997 أطلق عليها صحيفة الهمشري، ثم تبتها مجموعة من الصحف السيبرانية اليومية، منها: الأبرار، الأخبار، اطلاعات، إيران، أخبار إيران (باللغة الإنجليزية)، الجمهورية الإسلامية، كيهان، رسالات، والسلام، واتاحت لجميع المستخدمين فرصة الوصول الى المحتوى السيبراني لهذه الصحف السيبرانية.

أما وكالة الأنباء الإيرانية *IRNA* فقد لجأت الى شركة بريطانية أنشأت لها موقعاً للأخبار، مع توفير خدمة نقل مباراة الفريق الوطني لإيران مع الفريق السعودي عام 1997 عبر شبكة الانترنيت.

أسهم انبهار المؤسسات العلمية والحكومية، والقطاع الخاص، والشعب الإيراني بالعالم المتخيّل الذي يقيم في فضاء الانترنيت بانشغالهم عن مراجعة مدى ملاءمة المحتوى المطروح مع ثقافة الثورة الإسلامية والقيم المتشددة التي ينادى بها المحافظون، فبقيت الانترنيت لمدة عقد من الزمن بعيدة عن المراقبة، واستمر مستخدمي الانترنيت في رحلاتهم التخيلية بفضاء مفتوح، تجاوز المحددات والقيود الصارمة التي فرضتها الهيئات الدينية والسياسية على البوح بخطاب سياسي، أو ممارسة نشاط بات يتعارض مع أهل الحل والعقد في إيران.

بيد أن صحوة الإسلاميين المحافظين ونقدهم المستمر، والشديد للمحتوى المطروح في القنوات الفضائية، جعل الإدارة الحكومية تفكر بجدّية في تبني استراتيجية محلية للتعامل مع المحتوى الذي حفلت به مواقع الانترنيت، والذي يتعارض صراحة مع القيم الأخلاقية للثورة الإسلامية، كما أنه بات يشكّل منفذاً لتسلل أفكار الشيطان الأكبر (الولايات المتحدة) الى شريحة الشباب الذين لم تنضج منظومتهم العقدية الى المستوى الذي يجعلهم محصنين قبالة الهجمات الناعمة التي تسري في فيض مواقع الانترنيت وخدماتها الجاذبة.

وقد اختلطت (في بداية الأمر) إجراءات الحظر التي فرضتها سياسات شركة *TCI* في سبيل كف عمليات المنافسة التي مارسها القطاع الخاص بواسطة قناة الترويج لخدمة الانترنيت في المقاهي العامة الافتراضية *Cyber Cafe*، والتي حصلت في عام 2001[34]، مع الإجراءات اللاحقة، والتي أفرزتها السياسة الجديدة للدولة بحجب المواقع وتقطير مادة المحتوى السيبراني للكثير من المواقع، والتي بدأت بفرضها مع بدايات عام 2003. يضاف الى ذلك إلزام وزارة المعلومات وتقنيات الاتصالات للشركات المجهزة لخدمة الانترنيت بحظر جميع المواقع التي يستوطن في مادتها خطابات ومحتوى يتعارض مع أخلاقيات الثورة الإسلامية، أو المواقع التي تعارض النهج السياسي للثورة الإسلامية. حيث كانت هذه التعليمات عبارة عن مدونة تعهدات صورية في قائمة الموافقات الروتينية للشركات التي تنهض بمهمة تزويد خدمة الانترنيت في عموم البلاد، ولم تكن مستندة الى سياسة واضحة، أو استراتيجية قد صيغت فقراتها تحت أنظار المؤسسة الحكومية، أو المحافظين.

وبرر الباحث رحيمي (*Rahimi,2003*) عدم توفر الكوادر التقنية، والموارد المالية الكافية لدى الحكومة للتفكير بمثل هذه الاستراتيجية في ولاية الرئيس هاشمي رفسنجاني، الأمر الذي أجبرها على غضّ النظر عن المحتوى، وتجاهل بعض النداءات التي لم يعلو صوتها كثيراً بسبب عدم انتشار الخدمة خارج حدود المؤسسة الأكاديمية وشريحة محدودة

---

[34] . أقفل أكثر من 450 مقهى انترنيت بسبب استخدام خدمة الاتصال بخارج البلاد بواسطة خدمة *VoIP* والتي أثرت بشكل كبير على القيمة الاقتصادية المضافة التي حققتها شركة *TCI* على صعيد الاتصالات الدولية، فتوهم البعض أن هذه العملية كانت جزءاً من عملية المراقبة وحظر المواقع.

من المؤسسات الحكومية والقطاع الخاص، وشريحة من المثقفين الإيرانيين، وعدم بلوغ الفيض السيبراني الى حدود المؤسسات والمرجعيات الدينية المحافظة.

كذلك فإن اعتماد الحكومة لخيار التقليل من سرعة الخدمة (لكف عملية الوصول الى المواقع المحظورة) قد تعارض مع سعيها الى إدخال التقنية السيبرانية في كثير من الإجراءات الحكومية للتغلب على الإجراءات الروتينية، وترسيخ حضور بوابات الحكومة الالكترونية التي طالما عدتها جزءاً مهماً من سعيها الإصلاحي بالبلاد. لذا استمرت مهادنة الحكومة لفضاء الانترنيت مدة من الزمن تجاوزت عقداً من الزمان، ولم تفكر الحكومة بممارسة أنشطة الرقابة والحظر حتى اضطرت بفعل التحوّل الكبير الذي حصل على صعيد استخدام خدمة الانترنيت، وبعد أن تحوّلت من أداة لدعم الجهد البحثي والأكاديمي، باتجاه توسيع المدارك والاطلاع على ثقافة الآخر، ثم تحوّلت الى أداة ترفيهية، قبل أن تتحول الى أداة فاعلة للمعارضة السياسية، ومعارضة نهج الثورة الإسلامية ورموزها بصورة مباشرة، أو غير مباشرة.

2 .2 . الهيئات الشرعية والانترنيت:

حرصت حكومة إيران على توفير مناخ صحي ومنفتح لتوسيع دائرة أنشطة المؤسسة الدينية الإيرانية لنشر مذهب آل البيت من جهة، ونشر ثقافة الثورة الإسلامية وبصمتها على صعيد الإسلام السياسي، من جهة أخرى.

وسعت الى ترسيخ خطط طموحة لتنفيذ هذه الغايات وبالتنسيق المباشر مع الحوزات العلمية، والهيئات الشرعية، ووفرت جميع أشكال الدعم المالي والتقني لمثل هذه المشاريع، ومنذ العقد الأول من ولادة فضاء الانترنيت في إيران. من أجل هذا باشرت الحوزة العلمية وبقية الهيئات والمؤسسات الشيعية في إيران في احتضان عملية طموحة لتشكيل فضاء رقمي تسوده جميع تفاصيل العقيدة الاثني عشرية، وغذّته بمبادئ ثقافة الثورة الإسلامية ـ الإيرانية. ولم تقصر المساحة التي شملها الفضاء الجديد على الفضاء السيبراني الإيراني، وإنما سعت الى توسيع رقعته على عموم أقطار العالم الإسلامي، ومن ثم توسع باتجاه كافة دول العالم التي يستوطن فيها مجموعات، أو أفراد من الطائفة الشيعية، إيماناً منها بطبيعة المهمة الملقاة على المؤسسة الدينية في إيران بنشر ودعم الخطاطة العقدية في جميع بقاع الأرض، ولكي تقوم بالمهمة المقدسة في التمهيد لظهور الإمام المهدي.

ومن هذا المنطلق فقد وفرت تخصيصات مالية كبيرة، وسخرت جميع الطاقات العلمية والتقنية والشرعية في إيران، وخارجها، من اهل البيت الشيعي لإنشاء مواقع، تتسم بتقنيات عالية، وتضم محتوى رقمي ثري، وقنوات اتصال وتواصل مفتوحة مع المرجعيات لتحقيق هذه الغاية.

وقد حاولنا إجراء سلسلة من عمليات التنقيب السيبراني، على هذا الفضاء السيبراني المفتوح، وأثمرت تنقيباتنا بالكشف عن جزء من أنطولوجيا الويب الشيعية، التي تتلقى الدعم المباشر من حكومة الثورة الإسلامية، من مؤسستها العقدية في قم ومشهد وغيرها من الأماكن التي تتسم بأهمية خاصة على صعيد المذهب الجعفري. وقد سعينا الى تقسيمها وفق مواضيعها الى محورين، محور أساسي يجمع تحت جناحه مجموعة من المحاور الثانوية التي تلتحق بفضائه المعرفي ـ أنظر الجدول (2 - 2).

الجدول (2 - 2) ـ المواقع التي ترعاها الحوزة العلمية وغيرها من المؤسسات والهيئات الدينية الإيرانية على الانترنيت[35].

المحور الرئيسي	المحور الفرعي	عدد المواقع	اللغة
الرسول الكريم.	...	5	فارسي.
آل البيت عليهم السلام (335 موقعاً)	الامام علي.	20	فارسي ولغات أخرى
	فاطمة الزهراء.	14	فارسي ولغات أخرى
	الامام الحسن.	9	فارسي / عربي
	الامام الحسين.	21	فارسي ولغات أخرى.
	الامام السجاد.	3	فارسي
	الامام الباقر.	1	فارسي
	الامام الكاظم.	5	فارسي ولغات أخرى
	الامام الرضا.	7	فارسي ولغات أخرى
	الامام الجواد.	1	فارسي / عربي
	الامام الهادي.	7	فارسي / عربي
	الامام العسكري.	5	فارسي / عربي
	الامام المهدي.	122	فارسي ولغات أخرى
	ذرية آل البيت.	46	فارسي ولغات أخرى
	الأصحاب والرواة.	4	فارسي / عربي
	عام	70	فارسي ولغات أخرى
الأماكن الشيعية المقدسة (256 موقعاً)	الأماكن والمراقد.	56	فارسي ولغات أخرى
	الحسينيات.	86	فارسي ولغات أخرى
	المساجد.	114	فارسي ولغات أخرى
القرآن الكريم (127 موقعاً)	ترجمة القرآن.	4	فارسي
	تعليم القرآن.	33	فارسي / عربي
	تفسير القرآن.	7	فارسي ولغات أخرى
	علوم القرآن.	5	فارسي
	القرآن الكريم.	78	فارسي ولغات أخرى
	معلومات قرآنية.	1	فارسي
الحوزات العلمية.	...	115	فارسي ولغات أخرى
المعارف الشيعية (518 موقعاً)	الأخلاق.	13	فارسي ولغات أخرى
	الأدعية والزيارات.	15	فارسي ولغات أخرى

[35]. جمعت هذه البيانات من ادلة المواقع الإيرانية المتوفرة في فضاء الانترنيت . تاريخ الاستقصاء أكتوبر 2015.

المحور الرئيسي	المحور الفرعي	عدد المواقع	اللغة
	الاقتصاد الإسلامي.	1	فارسي
	التاريخ	6	فارسي
	الرجال والحديث	15	فارسي / عربي
	الطب الإسلامي.	4	فارسي
	العرفان الإسلامي.	3	فارسي
	العقائد الامامية	56	فارسي ولغات أخرى
	الفقه والأصول.	14	فارسي / عربي
	الفلسفة الإسلامية.	7	فارسي
	الفلك والنجوم.	3	فارسي
	معرف إسلامية.	367	فارسي ولغات أخرى
	المهدوية.	14	فارسي ولغات أخرى
أعلام إيرانيون (386 موقعاً)	القراء والحفاظ.	17	فارسي
	علماء الشريعة.	221	فارسي ولغات أخرى
	المدّاحون.	90	فارسي ولغات أخرى
	المراجع.	58	فارسي ولغات أخرى
الجهاد والشهادة (61 موقعاً)	الجهاد والشهادة.	7	فارسي
	الدفاع المقدس.	13	فارسي
	الشهداء.	41	فارسي ولغات أخرى
المراسم والشعائر (97 موقعاً)	الحج والزيارة.	15	فارسي ولغات أخرى
	مراسيم دينية.	19	فارسي ولغات أخرى
	محافل وملتقيات.	63	فارسي
	المآتم والهيئات الدينية.	221	فارسي
أماكن شيعية	...	36	فارسي ولغات أخرى

إن التغير المستمر في هيكلة مواقع الانترنيت، والتطور الآني في ولادة المواقع، أو اندثارها، يجعلنا في شك من أي محاولة لاستقصاء جميع المواقع، وأن ما نقوم به لا يزيد عن كونه مشهداً آنياً لمحتوى فضاء الانترنيت، يمكن أن نرسم من خلاله جزءاً محدوداً من المشهد السيبراني العولمي.

لذا يمكننا القول أن عملية البحث التي قمنا بها خلال النصف الأول من شهر أكتوبر 2015 قد أفرزت لنا حضور أكثر من 1932 موقعاً تخصصياً أعد على مستوى عال من المهنية، مع توفر محتوى داعم، وخدمات مميزة لدعم الخطاب الشيعي، والكثير من ممارساته العقدية.

كان للرسول الكريم 5 مواقع، وخصص لآل البيت مواقع مستقلة شملت الأئمة الاثني عشر (لم نجد موقعاً مخصصاً للإمام جعفر الصادق!) بلغ عددها 335 موقعاً، وخصص 256 موقعاً للأماكن المقدسة لدى الطائفة الشيعية، و115

موقعاً للحوزات العلمية، وخصص للمراسم والشعائر 97 موقعاً، و61 موقعاً للتحريض على الشهادة وترسيخ بصمات الشهادة في المذهب، بينما خصص أكثر من 386 موقعاً للمرجعيات الدينية، وأعلام المذهب الجعفري.

وقد أعدت مادة المحتوى بعناية بالغة، وانتخبت إضافة الى اللغة الفارسية لغات أخرى كالعربية، والأوردية، والانجليزية، والألمانية، والفرنسية، والروسية، والاسبانية، ولغات أخرى بحسب جنسية زوار المواقع المحتملين، ولضمان وصول البلاغات العقدية لجميع زوار هذه المواقع.

وبالوقت ذاته، فقد عمدت الى توطين هذه المواقع في جل بلدان العالم، لضمان توفر الخدمة السيبرانية خارج حدود إيران التي عانت وتعاني من حصار تقني شمل استضافة مواقعها في داخل حدود العالم الإسلامي وخارجه ـ أنظر الجدول (2 - 3).

الجدول (2 - 3) ـ التوزيع الجغرافي للمواقع التي ترعاها الحوزة العلمية والمؤسسات الدينية الإيرانية في عموم بلدان العالم[36].

ت	البلد	عدد المواقع	ت	البلد	عدد المواقع	ت	البلد	عدد المواقع
1	العراق.	87	17	تنزانيا.	13	33	نيجيريا.	2
2	روسيا.	1	18	تركيا.	1	34	النرويج.	2
3	فرنسا.	5	19	تايلاند.	1	35	الفاتيكان.	1
4	الأرجنتين.	2	20	الدانمارك.	8	36	هولندا.	7
5	أفريقيا الجنوبية.	1	21	سنغافورة.	1	37	الهند.	64
6	أفغانستان.	7	22	سوريا.	4	38	بنغلاديش.	1
7	ألمانيا.	21	23	السويد.	17	39	أذربيجان.	1
8	أستراليا.	19	24	السعودية.	20	40	ساحل العاج.	1
9	سكوتلاند.	1	25	عمان.	3	41	اليابان.	1
10	الامارات.	10	26	كندا.	55	42	شيلي.	2
11	أوغندا.	1	27	كينيا.	1	43	النمسا.	1
12	إيطاليا.	1	28	الكويت.	30	44	الولايات المتحدة.	82
13	إيرلندة.	1	29	لبنان.	47	45	بريطانيا.	96
14	البحرين.	57	30	بولندا.	1	46	اسبانيا.	3
15	بوتسوانا.	1	31	مدغشقر.	1	المجموع (813 موقعاً)		
16	باكستان.	130	32	ماليزيا.	1			

[36] . جمعت هذه البيانات من ادلة المواقع الإيرانية المتوفرة في فضاء الانترنيت . تاريخ الاستقصاء أكتوبر 2015.

وقد أثمرت تحرياتنا السيبرانية بالكشف عن 813 موقعاً وزّعت على 46 بلداً من بلدان العالم، وتراوح عديد هذه المواقع بين موقع واحد كما في: روسيا، وجنوب أفريقيا، وسكوتلاند، واوغندا، وإيطاليا، وايرلندة، وبوتسوانا، وتركيا، وتايلاند، وسنغافورة، وكينيا، والنمسا، واليابان، وساحل العاج، وأذربيجان، وبنغلاديش، والفاتيكان !.
بينما نلاحظ ارتفاع عدد المواقع وبلوغها بضعة عشرات في: العراق، والولايات المتحدة، وبريطانيا، ولبنان، والبحرين، والكويت، وكندا، والسعودية، والهند. بينما تفوقت باكستان على جميع الدول ببلوغ أعداد المواقع فيها 130 موقعاً.

2 . 3 . مقر الحوزة العلمية والانترنيت:

قامت معظم الهيئات والمؤسسات الدينية في إيران، والحوزة العلمية بمدينة قم بإنشاء مواقع لبث خطابها العقدي، ونشر ثقافة الثورة الإسلامية على مواقع الانترنيت، وأوغلت في توسيع مفردات حضورها بحيث شملت مواقع المرجعيات، والمدارس الدينية، والحوزات العلمية داخل حدود إيران وخارجها، ومواقع للفتوى، وأخرى لنشر الفقه الجعفري، ووكالات انباء الحوزة، واخبار الطائفة، بحيث رسخت لحضور افتراضي مكثف مناظر لحضور على التربة الإيرانية، الأمر الذي جعل مدينة قم مركز إشعاع وعاصمة تقنية المعلومات والاتصالات بإيران بحسب ما صرح به أحد أعضاء حكومة الرئيس خاتمي، مهدي خليجي عام 2005 (*Khiabany&Sreberny,2009*).

2 . 3 . 1 . الذاكرة السيبرانية للحوزة العلمية:

باشر مركز بحوث الحاسب للعلوم الإسلامية *Computer Research Centre for Islamic Sciences* في الحوزة العلمية بقم العمل على إدخال ورقمنة محتوى: خزائن الفقه الامامي، وخزانة التفسير وعلوم القرآن، وخزائن علوم الحديث دراية ورواية، مع الكثير من المصنفات التي تعنى بعقيدة الشيعة الاثني عشرية، إضافة الى خزائن تراجم وسير آل البيت، والأئمة المعصومين، وإدارة المحتوى السيبراني لهذه الخزائن العملاقة من خلال برنامج محوسب يدعم المستخدمين أثناء البحث عن النصوص، بواسطة آلة بحث موضوعي.
فبدأت حواجز القطيعة التي حرص على تشييدها أئمة المذهب الشيعي ومرجعياته العلمية، تضمحل وتتهاوى يوماً بعد يوم، بعد أن وجدوا في الآلة المبتدعة فضاءَ جديداً لحفظ تراث المذهب، وتسهيل عمليات البحث عن المواد الخصبة التي لم يكن قادراً على العثور عليها إلا الجهابذة منهم، وبعد بذل جهود مضنية لا تكاد تقارن مع نقرة آنية يمكن أن يمارسها المستخدم العادي لبلوغ أعماق الطبقات الجيولوجية لعلوم آل البيت المتوغلة الى أعماق تتجاوز بضعة عشر قرناً.
في البداية، اودعت المادة العلمية على أقراص ليزرية، وانتشر استخدامها في المكتبات العامة، والخاصة، ثم تناسلت نسخها، فبدأت تباع في المكتبات والأسواق. اعتبرت الحوزة هذا النشاط من الأمور المهمة التي تسهم بنشر العقيدة الاثني عشرية، داخل حدود العالم الإسلامي وخارجه، فشجعت طلبة الحوزة على المساهمة برقمنة المصنفات التي تحفل بها مكتبات الحوزة، وتحويلها الى محتوى رقمي ضخم، يمكن نشره في أقراص ليزرية، يسهل تداوله بين محبي آل البيت وأتباعهم حتى في الدول الإسلامية التي تمارس رقابة صارمة على هذه المادة التي لا يستحسنها أئمة المذاهب الفقهية في الأقطار الإسلامية التي يشيع فيها المذهب السني.
لم ينقضي النصف الأول من تسعينات القرن الماضي، حتى اكتملت عمليات زج الحواسب في مختلف مكاتب الحوزات العلمية، مع إدخال نظم محوسبة لإدارة الكثير من الأنشطة التنظيمية، والتعليمية فيها، وتغلغلت عمليات الرقمنة داخل حدود المؤسسة الأكاديمية للحوزة، وبدأت المرجعيات العليا تشجّع طلبتها على اتقان استخدامها، وتوظيفها لدعم عمليات نشر الخطاب العقدي الاثني عشري (*Mina,2010*).

مع بداية النصف الثاني لعقد التسعينات، بدأت خدمة الانترنيت بطرق أبوب مؤسسات الحوزة العلمية، فوجدت فيها المرجعيات الأداة التي طالما بحثوا عنها منذ عقود خلت لإيجاد أداة تنهض بمهمة نشر الخطاب الاثني عشري، وتحاول ايصاله خارج حدود الحوزة العلمية باتجاه بقية بلدان العالم الإسلامي، وغير الإسلامي على حد سواء.

ومع توسع دائرة حضور خدمة الانترنيت في عموم إيران، تناسلت مواقع كبار مرجعيات الحوزة العلمية، وآيات الله، والمرجعيات، وباشرت بخطاب متعدد اللغات[37] لضمان بلوغ مادتها الى طيف واسع من أشياع آل البيت. فأبصرت النور مواقع كل من: آية الله علي السيستاني، والشيخ جواد التبريزي، وعلي صنائعي، وحسين نوري همداني، ولطفي صافي جولبيجاني (*Mina,2010*).

وأصبح لكل مرجع من آيات الله الشيعة، بيتاً افتراضياً يزوره، باستمرار، أنصاره وأتباعه، لرصد ومتابعة ما يصدر عنه من فتاوى، ورسائل، واخبار ذات صلة بنشاطاته الدعوية، والعلمية، والاجتماعية. ويعد موقع آية الله حسين منتظري من المواقع ذائعة الصيت بين طلبة العلم، والمرجعيات العلمية الإيرانية، نظراً لما يضمه من مادة علمية، وفتاوى في النوازل الفقهية، واخبار نشاطاته العلمية والاجتماعية، بالإضافة الى وجود بريد الكتروني للتواصل مع هذه الشخصية العلمية، والحصول على إجابات علمية لمسائل متنوعة. ويحفل موقع الامام السبحاني الذي يقيم في موقع مؤسسة الامام الصادق بمحتوى رقمي مميز، ومواضيع متنوعة، ويضم مكتبة شاملة، مع مستودع للمقالات الإسلامية، وبوابة الى معهد الكلام الذي يلتحق بالمؤسسة ذاتها[38].

وقد قامت الحكومة، خلال الشهور الأولى من ولاية الرئيس محمد خاتمي، باستيراد أكثر من 200 ألف حاسب الكتروني لغرض توزيعها على الجامعات، والمعاهد العلمية، والمدارس المنتشرة بالبلاد. وكانت حصة المؤسسات الدينية والحوزات ما يقارب ربع هذه الكمية (أي حوالي 50 ألف حاسب) (*AA,2005*).

وسرعان ما تلقف طلبة المعاهد الدينية والحوزة العلمية في قم، هذه الحواسب، وشرعوا بتوظيفها في أنشطتهم الدراسية، والدعوية على حد سواء. بيد أن مدينة قم الصغيرة، والتي لا تتسع سوى لطلبة العلم الوافدين إليها من مختلف اقطار العالم الإسلامي، باتت تتسع هذه الأيام لاستضافة أكثر من 300 ألف حاسب، تنتشر في مؤسساتها الشرعية، وفي مساكن أهلها، وفي مكتبات علمائها، وكبار مرجعياتها العلمية.

وقد شجع التغلغل الحاسوبي في هذه المدينة على تناسل مقاهي الانترنيت التي جاوز عددها 200 مقهى رقمي يقصده الكثير من مواطنيها، وطلبة العلم، وفقهاؤها. ومنذ عام 2005 بلغ عدد مجتهدي الشيعة الذين يمتلكون مواقع على الانترنيت أكثر من 20 مجتهد بمدينة قم، على التوازي مع أكثر من 400 فقيه وأستاذ متمرس في الفقه الشيعي (*AA,2005*).

وقد تكاثرت مواقع الجيل الثاني من مجتهدي الشيعة ومفكريهم، واستوطنت في محتواها السيبراني المزيد من المسائل ذات الصلة بالنهج الإصلاحي، والمراجعات الفلسفية، ومناقشة مسائل ذات صلة بالمتغير السياسي، ونقد الواقع الإيراني. ومن هذه المواقع، موقع: سيد هادي خسروي شاهي، وحسن يوسف أشكوري، عبد الصاحب الخوئي، ومحمد ألاجوند، وأحمد الكاتب، وفاضل الميلاني، وغيرهم كثير (*AA,2005*).

---

[37] . بلغ عدد اللغات التي ينطق بها موقع أحد أئمة الشيعة المتأخرين، محمد فاضل لانكاراني أكثر من عشرين لغة!.

[38] . يمكن مراجعة الموقع على الرابط: *http://imamsadeq.com/*.

2 . 3 . 2 . المؤسسات الأكاديمية الشرعية:

احتضنت الحوزة العلمية والهيئات العلمية في قم الكثير من الجامعات التي توظف التقنية السيبرانية في إدارة العملية التعليمية، فهناك جامعة الامام الخميني الافتراضية *Virtual University* التي تسمح بالتسجيل الالكتروني وإدارة العملية التعليمية في رحابها السيبرانية ـ الافتراضية. كذلك توطنت في فضاء قم السيبراني، كلية علوم الحديث الالكترونية عام 2008، بعد أن كان مستقرها الأساسي في طهران، ثم التحقت بجامعة القرآن والحديث في قم[39].

ولقد أنشئت نسخة افتراضية للحوزة ومرجعياتها على مواقع الويب، وبدأت هذه المواقع تمارس دوراً مهماً تجاوز حدود حوزة قم، وغيرها من الحوزات العلمية، بعد أن انفتحت على فضاء رقمي، غابت عنه الحدود الجغرافية، ولم يعد أمام مستخدمي الانترنيت (من داخل حدود المؤسسة التعليمية بالحوزة، أو خارجها) حاجباً، ولا بوابة يضطرون للوقوف عندها بانتظار رؤية مرجعيتهم، وإمامهم الذي يقتدون به ويهتدون بهديه.

2 . 3 . 3 . ممارسة التدوين داخل حدود الحوزات العلمية:

ألقيت محاضرة تقديمية، في عام 2005، حول أنشطة التدوين السيبراني، في مدينة قم، وبإشراف مباشر من مكتب تشجيع المدونات الدينية *Office for the Promotion of Religious Blogs*، فالتحق برواد التدوين من طلبة الحوزة العلمية وبعض المرجعيات الذين بدأوا بممارسة التدوين منذ عام 2001 مجموعة كبيرة من المدونين المحافظين، وبدأ فضاء التدوين الحوزوي بالنمو تدريجياً، وتعمّقت جذوره في فضاء الانترنيت، فأضيفت قناة جديدة لنشر الخطاب الشيعي (*Mina,2010*).

وبدأت المدونات السيبرانية، ذات الطابع العقدي، بالانتشار في فضاء الانترنيت الإيراني، بعد أن سخّر الكثير من طلبة الحوزة العلمية، أنفسهم، لبث المذهب الشيعي الاثني عشري، والدعوة الى ثقافة الثورة الإسلامية، في محاولة لتحويل خطابها المحلي، الى خطاب إقليمي، يحاول الانفتاح على الفضاء العولمي، ولضمان بلوغ خطاب الثورة الى أبعد نقطة في فضاء الانترنيت المفتوح.

وبدأت المدوّنات الشيعية، بصبغتها الدينية، بالتوسع تدريجياً، حتى بلغ عدد المدوّنات الملتحقة بالخطاب الديني أكثر من 3,000 مدونة استمدت فيضها السيبراني من مضيف *Persianblog*. وقد انضمت أكثر من 3,000 مدوّنة شيعية أخرى بمضيف المدوّنات *Mihanblog.ir*. واستمر تناسل المدوّنات الشيعية، بحيث ظهرت حاجة ماسة الى إنشاء منصة المدونات الإيرانية *Parsiblog*[40] في بدايات عام 2005 لاحتواء الأعداد الكبيرة من المدوّنات ذات الطابع الديني، وتشجيع طلاب الحوزة العلمية، والمرجعيات على إنشاء مدوناتهم التي تهتم بالخطاب العقدي الاثني العشري، وتدعو الى الالتحاق بثقافة الثورة الإسلامية بإيران، والتعجيل بظهور الامام المهدي من غيبته (*Srebenry,&Khiabany,2008*).

ونتيجة لاقتناع الحوزة العلمية، في قم، بالدور الجوهري الذي يمكن أن تمارسه المدوّنات السيبرانية في بسط خطاطتها العقدية في فضاء الانترنيت، هرعت الى تأسيس مركز تنمية وتطوير المدوّنات السيبرانية، داخل حدود الحوزة، وباشرت بتوفير دعم سخي، مع تخصيصات مالية واسعة لتمويل هذا النشاط، على التوازي مع تشجيع طلاب الحوزة على المساهمة في إنشاء مدوناتهم، أو المساهمة مع المدوّنات العامة، مع الاهتمام ببث الخطاطة العقدية لولاية الفقيه التي جاء بها الامام الخميني.

---

39 . موقع الكلية : http://www.alhadith.ir.

40 . تجاوز عدد المدوّنات السيبرانية الفارسية في هذه المنصة على بضعة آلاف مدوّنة.

ثم تناسلت مدونات فرعية جديدة، فظهرت مدونات قرآنية، مثل مدوّنة: اسأل القرآن، والمنبر، والقرآن الكريم، والحكومة الإسلامية، والمذهب الشيعي الأمثل، والصحفيين المسلمين، وغيرها من المدونات التي لاقت إقبالاً كبيراً، وتوسعت مادتها المدونة (*Srebenry,&Khiabany,2008*).

ونتيجة للتوسع في أنشطة التدوين السيبراني ـ الديني، بعموم إيران، وضع حجر الأساس لاتحاد المدوّنين المسلمين والذي هرع للانتماء الى عضويته بضعة مئات من المدوّنين الإيرانيين خلال مدة قصيرة.

3 . الحضور السيبراني للمواطن الإيراني في فضاء الانترنيت:

لم تتأخر خدمة الانترنيت بالوصول الى المواطن الإيراني، فقد بدأت الخدمة ببلوغ شريحة محدودة في بدايات عام 1994، بيد أن حرص المواطن الإيراني على الإبحار في فضاء الانترنيت قد أسهم برفع عدد المستخدمين، بعد عقد من الزمان، الى أكثر من 10 ملايين مستخدم، وبنسبة تغلغل بلغت أكثر من 15 % من العدد الكلي للسكان. واستمر ازدياد عدد المستخدمين، سنة بعد سنة، فبلغ عدد المستخدمين 28 مليون مستخدم على أعتاب عام 2009، وبنسبة تغلغل ناهزت 38 % من العدد الكلي للسكان، مع بلوغ عدد المضيفات السيبرانية الى أكثر من 119,000 مضيف (*Koomen,2012*).

أسهمت الانترنيت في دعم شريحة واسعة من المستخدمين الإيرانيين، وفي ظل غياب عمليات الرقابة وحظر المواقع، على إنشاء مجتمع رقمي ـ متخيّل، في داخل المجتمع الإيراني، متجاوزة المحددات والقيود التي فرضتها معايير وقيم الثورة الإسلامية.

بدأت تباشير المجتمع السيبراني الجديد، وأرست جذورها في العاصمة طهران، مركز الثقافة المعرفة في البلاد، ثم بدأت تتسلل بطء باتجاه المدن التي تقاربها في الثقافة والتمدن.

ولم ينقضي عام 2003 حتى بلغ عدد مقاهي الإنترنيت في مدينة طهران أكثر من 1500 مقهى ازدحم كل منها بعدد كبير من الرواد الذين استوطنت أجسادهم المقاهي الجديدة، بينما حلّقت نفوسهم في الفضاء المتخيّل ـ المفتوح (*Koomen,2012*). وعلى التوازي مع مقاهي الانترنيت التي أنشأها القطاع الخاص كان هناك عدد كبير من مقاهي الانترنيت التي افتتحها شركة *TCI* في عموم البلاد. وكان الهدف من هذه المقاهي توفير مناخ آمن لاستخدام فضاء الانترنيت، مع حجب بصمة الثقافة الشيطانية والمخالفة لروح الثورة الإسلامية من التسلل الى باحة فضاء المستخدمين، والذين كان اكثرهم من طبقة الشيعة المحافظين، سواء من داخل مؤسسة الحرس الثوري الإيراني، أو الحوزات العلمية، أو ممن يحرصون على الالتزام الحرفي بثقافة وقيم الثورة الإسلامية بالبلاد.

وقد استثمر المستخدمون الإيرانيون القدرات الفريدة التي وفرها نظام Web 1.0 ونسخته المطورة Web 2.0 في إنشاء مواقع أخبار، والمشاركة بمختلف مفردات المعرفة، والمدوّنات السيبرانية التي أضحت تشكّل متنفساً للتعبير عن الرأي المعارض للخطاب السياسي، والثقافة التي جاءت بها الثورة الإسلامية بعيداً عن الرقابة الصارمة التي تمارسها الحكومة مع المطبوعات بمختلف أشكالها. ونجح المستخدم الإيراني بتوظيف ذكائه ومهاراته السيبرانية في إنشاء منصات لتداول الملفات، عبر المضيفات والخوادم المنتشرة بالبلاد، فنشر الكثير من الكتب والمطبوعات المحظورة، ونشر الموسيقى والألحان التي حاربت الثورة الإسلامية عملية نشرها في مجتمعها الجديد.

فتكاثرت الفضاءات المقيمة في فضاء الانترنيت بإيران، ولم يعد استخدام الانترنيت حكراً على طبقة المثقفين وخريجي الجامعة، بعد أن بدأ عامة الشعب الإيراني بالولوج الى الفضاء السحري لشبكة الانترنيت، سواء من خلال المساهمة بغرف الدردشة الالكترونية *Chat Rooms* او بممارسة مهنة الإبحار العشوائي في فضاء متصل لا تكاد تعثر فيه على نهاية مسدودة لا تأخذ بيدك نحو موقع جديد.

يمكن تقسيم بوابات تجهيز خدمة الانترنيت الى فئتين أساسيتين:

الفئة الأولى: بوابات الارتباط بواسطة الشبكات الأرضية.

الفئة الثانية: بوابات الارتباط بواسطة شبكات الهواتف المحمولة.

وتتباين نسبة الاقبال على كل فئة من هاتين، من محافظة الى أخرى بالمحافظات الايرانية ـ أنظر الجدول (2 - 4).

الجدول (2 - 4) ـ قنوات خدمة الانترنيت في المحافظات الإيرانية ـ عام 2015.

المحافظة	نسبة المساكن المرتبطة بخدمة الانترنيت	نسبة المواطنين الذين يستخدمون الانترنيت	عدد مستخدمي الانترنيت عبر الشبكة الأرضية	عدد مستخدمي الانترنيت عبر الشبكات المحمولة
أذربيجان ، الشرقية.	38.7 %	33.0 %	1,621,104	3,215,422
أذربيجان، الغربية.	35.5 %	25.3 %	1,228,610	2,324,649
أردبيل.	36.4 %	29.4 %	441,126	884,508
أصفهان.	43.1 %	34.2 %	2,389,422	4,870,221
البورز.	52.8 %	41.2 %	...	1,530,619
عيلام.	44.4 %	36.5 %	162,521	461,918
بوشهر.	46.0 %	41.7 %	327,850	1,096,487
طهران.	58.2 %	54.5 %	7,930,363	16,076,965
بختياري.	33.4 %	27.7 %	262,606	710,768
خراسان، الجنوب.	29.6 %	29.0 %	309,523	481,355
خراسان، رازاوي.	35.1 %	29.4 %	2,237,288	5,266,744
خراسان، الشمال.	28.3 %	22.8 %	259,039	591,600
خوزستان.	49.2 %	32.5 %	1,112,518	4,326,523
زنجان.	33.2 %	31.1 %	400,508	778,958
سمنان.	43.4 %	37.5 %	323,639	690,167
سيستان.	21.5 %	16.0 %	604,865	1,632,100
فارس.	44.2 %	36.9 %	1,607,788	4,407,047
قزوين.	36.1 %	31.7 %	453,942	1,061,867
قم.	53.0 %	42.8 %	491,126	1,056,872
كردستان.	28.0 %	24.3 %	537,413	1,198,305
كرمان.	32.8 %	27.7 %	941,925	2,371,838
كرمنشاه.	35.1 %	23.9 %	609,873	1,592,989
كوهجيلويه.	42.9 %	31.7 %	162,821	529,662
جوليستان.	32.1 %	25.2 %	643,922	1,473,488
جيلان.	35.5 %	26.6 %	1,104,013	2,463,350

المحافظة	نسبة المساكن المرتبطة بخدمة الانترنيت	نسبة المواطنين الذين يستخدمون الانترنيت	عدد مستخدمي الانترنيت عبر الشبكة الأرضية	عدد مستخدمي الانترنيت عبر الشبكات المحمولة
لورستان.	39.9 %	25.9 %	506,882	1,305,923
مازنداران.	47.0 %	35.8 %	1,715,530	3,494,871
ماركازي.	41.8 %	34.8 %	649,823	1,194,375
هرمزجان.	49.1 %	38.0 %	648,146	1,546,929
همدان.	37.2 %	31.7 %	613,117	1,358,403
يزد.	48.4 %	40.0 %	521,137	1,147,490
المجموع / المتوسط	42.9 %	35.1 %		

المصدر: *I.I.S.,2015*.

بصورة عامة، تصل أعداد المشتركين بخدمات الهواتف المحمولة الى حوالي ضعف المشتركين بخدمة الانترنيت عبر الشبكات الأرضية، وفي عموم المحافظات الإيرانية. وتتراوح نسبة المساكن المرتبطة بخدمة الانترنيت بين 21 % كحد ادنى في محافظة سيستان بينما تصل هذه النسبة الى قيمتها العليا في محافظة 58 % بمحافظة طهران.

3 . 1 . المواطن الإيراني والاقبال على خدمة الانترنيت:

يعد الشعب الإيراني من الشعوب المتعطشة لاستخدام الانترنيت، والمقبلين على استخدام الكثير من التطبيقات والخدمات المطروحة في فضائها المفتوح، والمكبّل على حد سواء.

بلغ عدد مستخدمي الانترنيت في إيران عام 2015 حوالي 25,017,850 مستخدم، شكل العنصر النسوي نسبة 35.1 % من عدد هؤلاء المستخدمين. بالمقابل، تباينت نسب استخدام الجنسين للانترنيت في المناطق الحضرية عن المناطق الريفية، فبلغت نسبة الذكور في المناطق الحضرية 56.9 %، بينما بلغت نسبة الإناث 43.1 %. أما في المناطق الريفية فبلغت نسبة مستخدمي الانترنيت من الذكور 65.4 %، وتراجعت نسبة الإناث الى 34.6 % (*M.o.ICT,2015*).

أما على صعيد التحصيل الدراسي، فبلغت نسبة مستخدمي الانترنيت من خريجي مراحل التعليم العالي 52.1 %، أما حملة الشهادة الثانوية فقد بلغت نسبة مستخدمي الانترنيت منهم حوالي 34.6 %، وبلغت نسبة مستخدمي الانترنيت من مراحل التعليم الأساسي المختلفة حوالي 12.6 %، بينما بلغت نسبة مستخدمي الانترنيت من فئة الذين يحسنون القراءة والكتابة 3 5، بينما تغلبت عليه فئة الأميين الذين بلغت نسبة من يستخدم الانترنيت منهم حوالي 4 % (*M.o.ICT,2015*).

حدثت طفرات غير مسبوقة على صعيد ازديا عدد مستخدمي الانترنيت في إيران، فتناسلت أعداد المستخدمين من 250 ألف مستخدم في عموم البلاد عام 2000 الى حوالي 47 مليون مستخدم عام 2015. وتصاعدت نسبة المستخدمين من العدد الكلي للسكان من 3.8 % عام 2000 الى نسبة ناهزت 57 % في عام 2015. وقد قفزت نسبة النمو في تغلغل الخدمة بالبلاد فبلغت ذروتها، في بدايات دخول الخدمة الى تخوم المجتمع الإيراني، وتهافت المواطنين للحصول على خدمة الانترنيت عام 2002 فبلغت النسبة 2100 %، بينما بدأت نسبة النمو بالتراجع تدريجياً نتيجة بلوغ حد الاكتفاء لدى شريحة واسعة من المجتمع فبلغت نسبة النمو بين عامي 2012-2015 حوالي 11 % ـ انظر الجدول (2 - 5).

الجدول (2 - 5) ـ عدد مستخدمي الانترنيت في إيران خلال السنوات 2000-2015.

السنة	عدد المستخدمين	عدد السكان	النسبة من عدد السكان	نسبة النمو
2000	250,000	69,442,905	3.8 %	...
2002	5,500,000	69,442,905	7.5 %	2100 %
2005	7,500,000	69,442,905	10.8 %	36.0 %
2008	23,000,000	65,875,223	34.9 %	206 %
2009	32,200,000	66,429,284	48.5 %	40 %
2010	33,200,000	76,923,300	43.2 %	3 %
2012	42,000,000	78,868,711	53.3 %	27 %
2015	46,800,000	81,824,270	57.2 %	11 %

المصدر: *IWS,2015*.

تعد إيران من أكثر دول الشرق الأوسط على صعيد عدد مستخدمي الانترنيت، إذ يشكّل عدد المستخدمين فيها حوالي 41.2 % من عدد مستخدمي الانترنيت في عموم بلدان الشرق الأوسط، وحوالي 1.1 % من العدد الكلي لمستخدمي الانترنيت على الصعيد العولمي ـ أنظر الجدول (2 - 6).

الجدول (2 - 6) ـ عدد مستخدمي الانترنيت في إيران بالمقارنة مع منطقة الشرق الأوسط والعالم في عام 2015.

المنطقة	عدد السكان	نسبة السكان من سكان العالم	عدد مستخدمي الانترنيت	نسبة مستخدمي الانترنيت من السكان	نسبة المستخدمين من العدد الكلي
إيران.	81,824,270	1.1 %	46,800,000	57.2 %	1.5 %
الشرق الأوسط.	236,137,235	3.3 %	113,609,510	48.1 %	3.7 %
بقية المناطق.	7,028,486,558	96.7 %	2,959,418,683	42.1 %	96.3 %
العالم.	7,264,623,793	100 %	3,073,028,193	42.3 %	100 %

المصدر: *IWS,2015*.

وتتباين دوافع الاستخدام لدى المواطن الإيراني بحسب مستوى تحصيله العلمي، وثقافته الشخصية، وطبيعة الحياة الاجتماعية التي ينتمي إليها، وانتماءاته العقدية والسياسية، والفئة العمرية التي يلتحق بها. وتشير الاحصائيات التي قامت بها المؤسسات العالمية الى أن شبكات التواصل الاجتماعي تستأثر باهتمام 82 % من المستخدمين في إيران، بينما تأتي متابعة الأخبار بالمرتبة الثانية وبنسبة 80 %، ولا تزيد نسبة الذين يمارسون اللعب عن 4 % بسبب بطئ الخدمة، وارتفاع كلفتها ـ أنظر الجدول (2 - 7).

الجدول (2 - 7) ـ دوافع استخدام الانترنيت في إيران.

المرتبة	قطاع الاستخدام	نسبة المستخدمين
1	شبكات التواصل الاجتماعي.	82 %
2	متابعة الأخبار.	80 %
3	التواصل.	67 %
4	أنشطة احترافية.	61 %
5	التدوين السيبراني.	47 %
6	تنزيل الملفات.	13 %
7	أعمال مكتبية.	13 %
8	ممارسة اللعب.	4 %

المصدر: *Abadpour&Anderson,2013*.

اما الاحصائيات التي أعلنتها وزارة تقنية المعلومات والاتصالات الإيرانية فقد جعلت من إقبال المواطن على التسوق الالكتروني بالمرتبة الأولى، وبنسبة بلغت 58.3 %، وتنزيل الملفات والصور والوسائط المتعددة بالمرتبة الثانية، وبنسبة بلغت 41.2 %، بينما وضعت المساهمة في شبكات التواصل الاجتماعي بالمرتبة السادسة وبنسبة لا تتجاوز 21 % ـ أنظر الجدول (2 - 8).

الجدول (2 - 8) ـ دوافع استخدام الانترنيت لدى المواطن الإيراني ـ عام 2015.

دافع استخدام الانترنيت	النسبة
الحصول على معلومات عن السلع والخدمات.	58.3 %
تنزيل ملفات معلومات وصور ووسائط متعددة.	41.2 %
إرسال أو استلام البريد الالكتروني.	37.5 %
تنزيل تطبيقات برمجية.	30.2 %
خدمات مصرفية الكترونية.	23 %
المشاركة بشبكات التواصل الاجتماعي.	21 %
البحث عن فرصة عمل.	8.3 %
الاتصال بالخدمات الهاتفية عبر الانترنيت.	6.7 %

المصدر: *M.o.ICT,2015*.

ولا تتوافق هذه الأرقام مع حجم الاقبال الهائل لعموم المستخدمين الإيرانيين على مختلف تطبيقات منصات شبكات التواصل الاجتماعي العولمية والمحلية. ويبدو أن هذه الأرقام قد أعدت بناء على ما يتوفر من مخرجات لنظم حجب المواقع وتقطير المحتوى السيبراني، والتي تغفل أو لا تستطيع تحديد حجم المستخدمين الذين يتجاوزون عقبة الحجب بآليات معلوماتية متنوعة.

ونظراً للرقابة الصارمة التي تمارسها الهيئات الحكومية والشرعية في عموم إيران على مستخدمي الانترنيت، فقد لجأ الكثير من المستخدمين الى الدخول الى فضاء الانترنيت من مساكنهم، أو مساكن الغير، فبلغت نسب الاستخدام في هذين المكانين 39 %، و7 %، على التوالي. وتأتي مقاهي الانترنيت بالمرتبة الثانية وبنسبة حضور بلغت 16 % وذلك لعدم التزام الكثير من أصحاب هذه المقاهي بسياسة الحجب الحكومية وتوفيرهم للمستخدمين أدوات رقيمة فاعلة لتجاوز مسألة الحجب. بينما تستخدم شرائح أخرى الانترنيت من خلال منافذ العمل، أو مؤسسات التعليم، أو المكتبات العامة ـ أنظر الجدول (2 - 9).

الجدول (2 - 9) ـ نسب مستخدمي الانترنيت في إيران بحسب موقع الاستخدام ـ خلال عام 2014.

موقع الاستخدام	نسبة المستخدمين
المساكن.	% 39
مقاهي الانترنيت.	% 16
مناطق العمل.	% 14
الأجهزة المحمولة.	% 14
المؤسسات التعليمية.	% 9
مساكن الغير.	% 7
المكتبات العامة.	% 1

المصدر: *Mohebali&Reza,2014*.

ويقبل المستخدم الإيراني على استخدام مجموعة متنوعة من الخدمات والمواقع التي تتوفر فضاء الانترنيت في إيران.
وتلعب عملية حظر المواقع وحجب المحتوى السيبراني في إعراضه عن بعض المواقع لصعوبة الوصول إليها، كما تولّد لدى بعض المستخدمين رغبة قوية في الوصول اليها لإشباع رغبة استكشاف المحتوى الممنوع، فيسعون الى توظيف أدوات تدعم فرصة اجتيازهم جدران الكف السيبراني.
بيد أن السعي الحثيث للإدارة السيبرانية في الحكومة الإيرانية على إيجاد تطبيقات بديلة للخدمات المحظورة قد أسهم في تلبية جزء لا يستهان به من حاجات المستخدم الإيراني من الخدمات السيبرانية والتواصلية، ولو بجودة أقل من تلك التي توفرها التطبيقات والخدمات المتوفرة لجميع المستخدمين.
وأظهرت الاحصائيات التي أجرتها مؤسسة *Small Media Organization* من خلال تتبع أنماط ونزعات استخدامات المواطن الإيراني، أن أكثر عشرة ومواقع انجذب اليها هؤلاء المستخدمين خلال عام 2014، سواء الخدمات العولمية أو الخدمات الإيرانية البديلة، أن مواقع التواصل الاجتماعي قد احتلت الجزء الأعظم من اهتمامات المواطن الإيراني (المراتب:1 ، 2 ، 3)، بينما جاءت بعدها الخدمات الداعمة لتطبيقات الهواتف الذكية الحواسب اللوحية (المراتب: 6، 9، 10). وقاربتها بالإقبال التطبيقات الداعمة لتصفح مواقع الانترنيت، والتي قد يستخدم بعضها لبلوغ مواقع الفئتين السابقتين في كثير من الأحيان (المرتبتين: 5، 7) ـ أنظر الجدول (2 - 10).

الجدول (2 - 10) ـ أكثر المواقع والخدمات السيبرانية التي يقبل عليها المستخدم الإيراني في الانترنيت.

المرتبة	المواقع والخدمات الإيرانية	المواقع والخدمات العولمية
1	Cloob, Facenama	Facebook
2	Aparat	You Tube
3	Dialog	WeChat
4	Lenzor	Instagram
5	Saina	Firefox
6	BeepTunes	iTunes Store
7	Parsijoo	Google
8	Webgozar	Google Analytics
9	Café Bazaar	Google Play
10	Sibche	App Store

المصدر: *Small-Media,2014*.

وتكاد تتوافق هذه النزعات في الاستخدام مع نزعات الاستخدام على المستوى العولمي، بيد أن ما يميزها هو انشطار المستخدم الإيراني، بين تطبيقات عولمية، وأخرى محلية، نتيجة لسياسة الحجب التي تستخدمها الحكومة، وتناوب حكم الحظر والسماح على هذه الخدمة أو تلك بحيث يبقى المواطن في حالة تأرجح بين الاستمرار بالخدمة أو العزوف عنها بصورة مؤقتة أو دائمة.

بصورة عامة، تتدرج ثقافة استخدام الانترنيت بين عدة مستويات، وينصبغ كل مجتمع من مجتمعات المعلومات المعاصرة بصبغة ثقافة الاستخدام التي يتميز بها أفراده. وذهب الكثير من المتخصصين الى أن عدد المستخدمين، ونسبتهم من عدد السكان لا تعد مؤشراً على نمو قدرات أفراد المجتمع على توظيف أدوات المعلومات واستغلالها على صعيد التنمية المستدامة بالبلاد.

وقد اقترحت مؤسسة *Open Research Network* ثلاثةأربع مستويات لتحديد مرتبة ثقافة استخدام الانترنيت في مجتمعات المعلومات المعاصرة (*ORN,1999*) :

المستوى البدائي: يسعى المستخدمون في هذه المرتبة الى توظيف خدمات الانترنيت وتطبيقاتها المختلفة في مجالات تقليدية وعبر تطبيقات شائعة وغير متخصصة.

المستوى التقليدي: يسعى المستخدمون في هذه المرتبة الى إجراء تعديلات على صعيد الممارسات لتوطين تطبيقات الانترنيت بحيث تلبي الحاجات القائمة داخل حدود المجتمع. فتستخدم الانترنيت (بصورة مباشرة) لتعزيز أنشطة الأفراد والمجتمع في مختلف قطاعات الأنشطة، والتقليل من حجم الانفاق لدعم عجلة الاقتصاد. ويعد شيوع هذا المستوى من الاستخدام مؤشراً على بدايات ترسيخ جذور الفضاء السيبراني وتطبيقاته في المجتمع.

المستوى التحويلي: يباشر أفراد المجتمع الذي يستخدم فضاء الانترنيت وتطبيقاته في إنشاء تطبيقات جديدة لإحداث تغييرات ملموسة في الممارسات والعمليات التي تسري داخل حدود المجتمع. إن التطوير الذي يمارس ضمن هذه

المرتبة قد لا يرتقي في كثير من الأحيان الى مستوى المعايير التقنية المناظرة للتقنية السائدة في البلدان النامية بيد أنه يلبي لحد ما الحاجات القائمة في المجتمع.

المستوى الابتكاري: في هذه الحالة يسعى أفراد المجتمع الى توظيف الانترنيت واستثمار القدرات السيبرانية التي تستوطن في فضائها بنهج يتسم ببصمات ابتكارية تدعم عمليات انتقال حاسمة على الصعيد التقني، وترسخ لعمليات نمو متلاحقة ومستدامة، الأمر الذي يمنح قطاع تقنية المعلومات والاتصالات القدرة على ترسيخ حضورها القتي على المستوى العولمي والمباشرة بالدخول في شراكات مع الشركات العملاقة لتطوير التطبيقات والخدمات والأدوات.

عمد فريق مؤسسة *Open Research Network*، في دراسته التي أعدها عن إيران عام 1999، الى عد مجتمع المعلومات في إيران ضمن المستوى التقليدي، وأن استثماره للانترنيت لا يخرج عن حدود توظيف التطبيقات الشائعة في تسيير دفة الأنشطة السائدة بالمجتمع، أو الإسراع بتنفيذها (مثل خدمة البريد الالكتروني قبالة خدمة البريد التقليدي، أو النشر المكتبي قبالة عملية الطباعة التقليدية) (*ORN,1999*).

من جانبنا نرى أن الصورة قد تغيرت مع العقد الأول من الألفية الجديدة، وأن إيران قد نجحت بتحقيق قفزة نحو المرتبة التي تليها (المستوى التحويلي) على صعيد المجتمع، بصورة عامة، بيد أن هناك الكثير من المؤسسات العلمية والتقنية قد بدأت بتلمّس حافات المستوى الابتكاري.

3 . 2 . فضاء المدونات الإلكترونية:

يمكن وصف المدونة الإلكترونية[41] *Weblog* بأنها عبارة عن صفحة ويب، توفر لمستخدميها فرصة التعليق المباشر *On-Line Commentary* مع إمكانية تحديثها بصورة دورية من قبل صاحبها، وعرضها وفق الترتيب الزمني للنصوص المضافة إليها.

انفتح فضاء المدونات الالكترونية *Weblogestan* على الحضور السيبراني للشبيبة الإيرانية في بداية شهر سبتمبر من عام 2001 على يد سلمان جريري (*Mina,2010*)، بعد ان أصبحت عملية التدوين باللغة الفارسية ممكنة في فضاء الانترنيت، ولم يمر سوى عامين حتى احتلت اللغة الفارسية المرتبة الرابعة بين اللغات السائدة في فضاء التدوين السيبراني ـ العولمي (*Khiabany&Sreberny,2007*). ويعد الصحفي الإيراني حسين ديراخشان الرائد الأول على صعيد دعم انتشار وتناسل المدونات الإلكترونية في إيران. فقد أنشأ مدونته الأولى (الناطقة باللغة الفارسية) في شهر سبتمبر من عام 2001. ولضمان أن تؤتي بذرته الأولى ثمارها أودع في مواقع الانترنيت دليلاً رقمياً باللغة الفارسية لتعليم أبناء بلده كيفية إنشاء مدوناتهم الشخصية بلغتهم الأم(*Berkeley,2006*).

واستمرت عملية التوسع في هذا الفضاء ليتحول شيئاً فشيئاً الى مجال احتوى حضوراً افتراضياً لعدد كبير جداً من المدوّنين الذين التحقوا بمجتمع جديد، اتسم بالانفتاح على العالم، وغياب القيود الصارمة التي تفرضها الحكومة على مواطنيها وتمنعهم عن التعبير بحرية، فتنوعت هوية أفراد المجتمع السيبراني الجديد، فالتحق به الصحفيون، والمثقفون، والسياسيون، ولم يجد بدأ الحوزويون وطلبة المدارس الدينية من ممارسة حرفة التدوين أسوة ببقية

---

[41] . تعرّف المدونة *Weblog* والتي شاع اختصارها بالمصطلح *Blog* بأنها عبارة عن جريدة أو مذكرات يومية مودعة بصورة مباشرة على مواقع الانترنيت. وقد صممت مواقع المدوّنات بحيث تظهر المواد التي يتم يدخلها المدوّن مرتبة زمنياً، مع منحه فرصة نشر محتوى مادته على المساحة الهائلة التي تمتد عليها الشبكة العنكبوتية العالمية *WEB* .

لا تخضع المدوّنات الإلكترونية الى قواعد نشر محددة تنتظم على أساسها النصوص المودعة فيها، ولا توجد جهة تراقب ما يرد فيها، مما يمنح أصحابها فرصة ثمينة للبوح بكل ما يجول في خواطرهم، وتبادل الآراء مع الغير، وترسيخ حضورهم على العقد الشبكاتية للانترنيت بوصفهم موارد مرجعية لنشر المعلومات، متجاوزين جميع أنماط القيود التي المفروضة في المجتمع التقليدي عبر هيئاته السياسية والمجتمعاتية.

المجتمع، ولاستثمار هذه الأداة الجديدة في سد فراغ قد تتفاقم مساحته نتيجة كثرة تناسل مدونات التيار المناهض فيه (*Rigby,2007*).

وقد ازدادت ألفة المستخدمين الإيرانيين بفضاء التدوين، فتحوّل الى ساحة للتواصل مع الآخر، داخل حدود إيران وخارجها، وللتفاعل مع الحدث والتعبير عن انعكاسات الأحداث على الفرد والمجتمع، والحوار مع المعارضين، وتوجيه النقد لكل المظاهر التي تحصل هنا او هناك، دون إحساس بمضايقة أو حرج كالذي يجده على أرض الواقع الصلبة، والمحددات الحازمة التي لا تقبل برأي مناهض ولا نقد بنّاء (*Cohen&Krishnamurthy,2009*).

ورغم تباطؤ خدمات شبكة الانترنيت (في عموم إيران) نتيجة للطوق الذي تفرضه آليات المراقبة السيبرانية التي تمارسها الحكومة الإيرانية على هذه الخدمة ، يحرص المدوّنون الإيرانيون على تحديث مادة مدوّناتهم يوماً بيوم. وتظهر عناوين المدوّنات (التي استعيرت من التراث الشعري الفارسي) بجلاء سمات المعارضة والاحتجاج لأصحابها إزاء الواقع الذي يشخص أمامهم بقوة، مثل : مدوّنة هايشيستان (أرض بلا رجال)، ومدوّنة باينيشاني (اللا مكان)، ومدوّنة خاكي غريب (أرض العزلة)، ومدوّنة أفكاري خصوصي (الأفكار الخاصة).

لم يقارب عام 2001 على نهايته حتى بلغ عدد المدونات الناطقة باللغة الفارسية أكثر من مائة مدونة، بينما تزايد عددها فبلغ بضعة عشرات آلاف مدونة مع حلول عام 2002، وقد تجاوز عددها عام أكثر من مائة وأربعين ألف مدوّنة نشطة تقيم في فضاء تدويني بلغ عدد مدوّناته 700 ألف مدوّنة في عام 2003 (*Parsa,2008*) ـ أنظر الجدول (2 - 11).

الجدول (2 - 11) ـ أكثر عشرة مدونات إيرانية نشطة في عام 2003.

منصة التدوين	عدد المدوّنين	نسبة المساهمة %
blogspot.com	60,642	21.85
persianblog.com	20,440	7.37
blogdrive.com	17,831	6.43
modblog.com	14,785	5.33
livejournal.com	10,518	3.79
20six.fr	6,422	2.31
myblog.de	4,988	1.80
nikki-k.jp	3,630	1.31
co.uk	3,434	1.24
cocolog-nifty.com	3,172	1.14
المجموع	145,862	...

المصدر: *Khiabany&Sreberny,2007*.

وقد أثار فضاء المدّونات الإلكترونية ـ الإيرانية اهتمام عدد كبير من الباحثين في الولايات المتحدة وأوربا، فتناولوه بالدراسة والتحليل وفق نهج معلوماتي صرف، أو من خلال معالجات سياسية، وأخرى ذات طابع اجتماعي.

أظهرت هذه الدراسات وجود أربعة محاور رئيسة تتقاسم المساحة السيبرانية التي تمتد عليها هذه المدّونات. ويتميز كل قطب من هذه الأقطاب بخصائص بنيوية، تميزه، وتحدد ملامح المادة المطروحة في مدوّناته، والسمات التي تحدد

معالم شخصيات المدوّنين الذي يودعون خطابهم في بيئته الشبكاتية. وقد قسّم الباحثان (*Kelly &Etling,2008*) هذا الفضاء الى أربعة عناقيد أساسية:

العنقود الأول: مدوّنات الشعر والشبكات المنوّعة:

يتميز هذا النمط من المدوّنات الإلكترونية بخلوه من الصبغة الأيديولوجية، وتتألف مادته السيبرانية من مجاميع متراكبة من المدوّنات التي تمتد مادتها على طيف واسع من المواضيع المتنوعة(كالثقافة، والفنون، والرياضة، والزرادشتية،وأمور أخرى يصعب حصرها)، بالإضافة الى معالجتها لمسائل الشعر والشعراء وعلى بعد زمني يشمل تاريخ فارس العريق وامتداداته في الأزمنة الحديثة.

وتلتحق بهذا المحور مجموعة متنوعة من المدوّنات الشعبية التي لا تنتمي الى التيارات السياسية والثقافية الكبيرة والمشهورة بالبلاد، أو تلك التي ترتبط بها رابطة الشباب أو المثقفين الايرانيين.

العنقود الثاني: مدوّنات الفئات الإصلاحية والعلمانية:

تتألف مدوّنات هذا المحور من تجمّع واسع يضم تشكيلة متنوعة من المدوّنات التي تنتظم ضمن نسيج ثري من فضاء المدوّنات الإيرانية التي أنشأتها مجاميع من المدوّنين الذين ينتمون الى شخصيات إصلاحية، وأخرى تنتمي الى التيار العلماني. وتقيم شريحة واسعة من مدوّني هذا المحور خارج إيران ممن ينتمون الى تيارات سياسية وإصلاحية معارضة غادرت البلاد في السنوات الأخيرة.

ويشخص أمامنا في ساحة هذا المحور نمطين أساسيين من المدوّنات:

النمط الأول: مدوّنات يعكف على إعدادها مغتربون علمانيون يسعون للدفاع عن حقوق المرأة، ويدعون الى إطلاق سراح سجناء مودعين في سجون الحكومة الإيرانية. وهناك مدوّنات أخرى يناقش أصحابها مسائل محظورة في ساحة المتغير الثقافي في ظل هيمنة الحكومة الإيرانية مثل: مسائل تخص الثقافة العالمية، والسينما، والصحافة الحرة، والنقد.

النمط الثاني: مدوّنات تعود الى سياسيين يتمتعون بنزعة إصلاحية تعالج مدوّناتهم مواضيع ساخنة في إيران مثل : التجاذبات السياسية في البلاد، وإساءة معاملة المنتمين الى التيارات الإصلاحية، وعدم عناية النظام بالبيئة المحلية، وغيرها من المسائل الساخنة التي تستأثر باهتمام العامة والخاصة على حد سواء.

العنقود الثالث: مدوّنات التيارات الإسلامية المحافظة

يشكل التيار الذي يساهم في إعداد مادة هذه المدوّنات مجموعة متنوعة من الجهات التي ترسّخ الخطاب الديني الذي ترفع رايته الثورة الإسلامية بإيران، وتلك التي تصدع بخطاب العقيدة الشيعية ـ الإمامية وتدعو بقوة الى سيادة ولاية الفقيه في أرجاء البلاد، وعموم رقعة البلاد الإسلامية. ويضم هذا المحور مدوّنات قطاعية مثل:

مدوّنات السياسات المحافظة (*ConPol*) حيث نجد في خطابها المطروح على الانترنيت مجموعة متنوعة من النقاشات والنقد الذي يمارسه المدوّنون تجاه السياسيون وما يمارسونه من سياسات في عموم البلاد. ورغم أن جلّ ما يدوّن في هذا القطاع يصبّ في دعم الحكومة الإيرانية، فلا تخلو مادتها في بعض الأحيان من نقد موجّه الى المؤسسات الحكومية، والقيادات السياسية بخطاب سياسي مبطن.

مدوّنات المذهب الاثني عشري (*12er*) التي تعدّ المورد الجوهري للمذهب الشيعي الذي يدين به مسلمو إيران، ونظامهم السياسي. ونجد في مادة هذه المدوّنات الحنين الروحي الذي يلتهب في قلوب الإيرانيين ويشدّهم بقوة الى التنقير عن علامات ظهور الإمام المهدي الذي سينتشل البشرية من غياهب الضلال. لقد بذل الرئيس الإيراني احمدي نجّاد ما في وسعه لترسيخ أسس هذه المدوّنات ليكسب ثقة التيار المتطرف، ويجعل منه مورداً لهذا النمط من الخطاب المتشدّد الذي يشدّ أزر سلطته السياسية بالبلاد.

مدوّنات الشباب المتديّنين (***relYth***) الذين ينتمون الى الأندية الشبابية والطلابية في المدارس والجامعات، ممن يميلون الى التيار الديني المتشدّد كنتيجة لما يحفل به المجتمع الإيراني من تيارات ومدارس تؤسس الخطاب الديني، وتعزّز وجوده في جلّ تفاصيل الحياة اليومية.

العنقود الرابع: مدوّنات متنوعة

ويضم في فضائه مجموعة متنوعة من المدوّنات السيبرانية التي انبثقت عن مادة العناقيد الثلاثة السابقة، بيد أن مضامينها قد توزعت بنمط يمنع من الحاقها بها. فجل مضامينها مشتتة ولا تنتمي الى تيار فكري أو أيديولوجي محدد، وتفتقر الى مضامين مشتركة يمكن إلحاقها بها. فاهتم مدونوها بالرياضة، او الوسائط المتعددة، أو مسائل ذات صلة باهتمامات الأقليات الدينية أو الاثنية في إيران.

في البداية كان فضاء المدوّنات السيبرانية أكثر الأماكن اماناً لمن يريد بثّ ما يجول بخاطره، ويمتلئ رغبة في تحقيق إصلاح سياسي، والدعوة الى تقليل القيود الصارمة التي تفرضها المؤسسة الدينية. من أجل هذا هرعت نسبة كبيرة من مستخدمي الانترنيت، بإيران، الى هذا الفضاء المفتوح والخالي من القيود والرقابة، للتعويض عما تعاني منه بسبب غياب القدرة عن التعبير عن الرأي المناهض والناقد لمعاناة المواطنين في حياتهم اليومية.

وبالوقت ذاته، هرع طلبة المؤسسات الدينية، والحوزات الى إنشاء مدوناتهم التي اقتصر خطابها على الترويج للخطاطة العقدية والسياسية للثورة الإسلامية، والمذهب الاثني عشري. وبالوقت ذاته استثمر رجال الصحافة والاعلام هذا الفضاء لإنشاء مدوناتهم الإخبارية والسياسية بعيداً عن القيود التي فرضتها مؤسسات الاعلام المسيسة وخطاب ثقافة الثورة الإسلامية الذي استرشدت به لمواجهة أي محاولة مناهضة بالإقصاء أو العقوبات الزاجرة.

لعل من أوائل المدونات ذات الصبغة الدينية، والتي دشّنت حضور الشخصيات والرموز السياسية والمرجعية في إيران، هي مدونة حجة الإسلام محمد علي أبتاهي (نائب رئيس الجمهورية الإيرانية السابق محمد خاتمي)، والتي دشنها بتدوينته الأولى في عام 2003 . عكست التدوينة السياسية الأولى في فضاء التدوين الإيراني، حساً مرهفاً، وشفافية في ا لإفصاح عن الهوية، والقاء الضوء على الأحداث السياسية التي تدور في البلاد بعيداً عن التكلّف، وبث الكثير عن حياته اليومية، والمهنية، الأمر الذي جذب عدداً كبيراً من المتابعين من داخل إيران وخارجها.

ومارس الخطاب المعتدل في هذه التدوينة، والنجاح التي حققته في فضاء المدونات الإيرانية والعولمية الى تشجيع شريحة واسعة من طلبة الحوزة وبقية المؤسسات والمعاهد الدينية الشيعية بالبلاد على إنشاء مدوّناتهم الشخصية التي اتسمت بصبغتهم الدينية المميزة. فبدأ فضاء المدونات المحافظة والدينية بالنمو التدريجي ضمن عناقيد المدونات الإيرانية التي استوطنت فضاء *Weblogestan* وتعددت هوية المشاركين بهذا العنقود، وتباينت انتماءاتهم وهوية المرجعيات التي يدينون لها بالولاء، إلا أن توجهاتهم كانت متوافقة بالدعوة الى ثقافة الثورة الإسلامية، والمذهب الاثني عشري، وبيان محاسن المرجعيات الشيعية، والرد على الفرق الإسلامية المخالف. وقد تكاثرت فروع هذا العنقود التواصلي وأطلق على أصحابه **الطلبة** كونهم طلبة ملتحقين بالمؤسسة الدينية والحوزات العلمية *Talabeh-I Az Nasl-E Sevom* (*Amir-Ebrahimi,2010*).

وقد أدى التوسع الكبير في عدد مدونات الطلبة، وتنوع مسارات الخطاب الشرعي والسياسي المطروح في مادتها السيبرانية الى تزايد القلق لدى المرجعيات وإدارات الحوزة العلمية، من إمكانية توسع دائرة المشاركة أو انفتاح الطلبة على تيارات مناهضة على الصعيد السياسي، أو تتبنى نهجاً يخالف خطاطة الحوزة المعرفية، الأمر الذي قد يشكل خلخلة في المنظومة العقدية، أو القناعات السياسية لدى شريحة من الطلبة. لذا أجبر خطاب الطلبة المدونين

على الالتزام المطلق بخطاطة الحوزات، والمرور القسري من خلال قنوات الرقابة والمراجعة الحكومية التي تسترشد بتوجيهات الحرس الثوري وتنصاع الى سلطته القاهرة.

وقد عمدت الحوزة عام 2006 الى تأسيس مكتب في قم يعنى بمتابعة هذه المسألة وتطوير محتوى المدونات الشيعية ذات الصبغة الحوزوية، أطلق عليه مكتب المدونات الدينية الالكترونية *Daftar-e Tose'eh-ye Weblog-haye Dini*. وتوسعت نشطات المكتب وتوجهت نحو متابعة مدونات طالبات الحوزة، وأنشأت لهن عام 2007 مدونة أطلق عليها "**مدوّنة الأخوات**" (*Amir-Ebrahimi,2010*).

وعلى صعيد متصل يلاحظ أن فضاء المدوّنات بإيران قد التصقت به سمة السجال السياسي المحموم بعد أن شاركت الحكومة مواطنيها في احتلال الرقعة السيبرانية للانترنيت لتباشر أنماطاً متنوعة من المواجهات التي يسودها خطاب سلطوي وخطاب مناهض بالوقت ذاته.

لعبت المدوّنات السيبرانية في إيران دوراً فاق الدور الذي تمارسه منظمات المجتمع المدني *NGO* في بلدان أخرى، وباتت تشكّل ضغطاً متزايداً على الحكومة الإيرانية التي أضحت تستشعر مدى خطورة الدور الذي تمارس في إعادة تشكيل الأنساق المفاهيمية للشبيبة الإ يرانية، وتوحّد صفوف التيارات السياسية المعارضة، فهرعت الى توظيف جميع الآليات السيبرانية المتاحة لسد جميع الثغرات التي بدأت تتعمق في كيان النظام الذي استغرقت ثلاثة عقود لإرساء أركانه.

ولمجابهة السيل الهائل من المدوّنات السيبرانية للمعارضة الإيرانية توجهت الحكومة الإيرانية الى تبني خطة لتجنيد أكثر من 10 آلاف من عناصر الباسيج كمدوّنين من العاملين ضمن جناح الحرس الثوري الإيراني لشحن فضاء المدوّنات الإيرانية بخطاب يدعم الخطاب السلطوي، ويرسّخ مبدأ تهافت الخطاب المعارض للسلطة عبر توظيف مبادئ العقيدة الاثني عشرية بطريقة تجعل من المعارض خارجاً عن الملّة الشيعية ولا يخدم إرهاصات ظهور إمام الزمان(*Kelly& Etling,2009*).

3 . 3 . حضور المواطن الإيراني في شبكات التواصل الاجتماعي:

منذ ولادة منصات شبكات التواصل الاجتماعي، وما تلاها من ظاهرة تناسل تطبيقاتها التواصلية المتعددة، أولع الشعب الإيراني بتوظيف هذه التطبيقات لتوطيد صلاتهم مع عوائلهم، المقيمين في إيران وخارجها، ومع أصدقائهم وزملائهم. وقد وجدوا في فضاء التواصل المفتوح فرصة للإعلان عن آرائهم، وبيان معارضتهم لممارسات الحكومة، أو بعض مفردات ثقافة الثورة الإسلامية، أو الالتحاق بتيارات سياسية معارضة.

وقد استخدمت جميع شرائح المجتمع، ومؤسساته الحكومية، والمرجعيات، والتيارات السياسية، ومرشحي الانتخابات فضاء التواصل الجديد، فتزاحمت نصوص الخطابات المطروحة في هذا الفضاء الاتصالي، بحيث بدأت المؤسسات الأمنية، وعلى رأسها الحرس الثوري التي شعرت بالقلق من الخطاب الذي يموج به الفضاء التواصلي السيبراني، غير أن ناقوس الخطر قد دقّ بعنف مع الأحداث التي عصفت بالبلاد قبيل وبعد الحملة الانتخابية لعام 2009 فتوفرت الفرصة المناسبة لحظر الخدمة من قبل الحكومة وبمباركة مباشرة من المرجعية التي عدّت بوابة منصات التواصل الاجتماعي منفذاً لتسلل الريح المناهضة للثورة الإسلامية عبر القنوات التي سخرها الغرب للمواجهة الناعمة مع الثورة الإسلامية في إيران (*Rafizadeh&Alimardani,2013*).

ورغم الحظر الذي تبنته الحكومة، وايغالها بإصدار عقوبات رادعة تدرجت بين أحكام بالسجن الى الإعدام بحق مستخدمي هذه المواقع متى ناهضت بصورة علنية النظام أو مؤسساته الشرعية، فلم ينصرف الكثير من الإيرانيين عن ممارسة أنشطة التواصل باستخدام قنوات التسلل السيبراني، والتحايل على عمليات الحظر. وقد اضطرت الحكومة

للتخفيف من حدّة الغليان الشعبي إزاء عمليات الحظر لمواقع التواصل الاجتماعي فخصصت حجماً كبيراً من التخصيصات المالية لإصدار تطبيقات بديلة للتواصل الاجتماعي، تتسم بانتظامها بقواعد ثقافة الثورة ومبادئها، اقتنع البعض بالتحول إليها، بينما بقيت شريحة كبيرة ملتحقة بفضاء التواصل العولمي، ومن خلال قنوات التحايل السيبراني ـ أنظر الجدول (2 - 12).

الجدول (2 - 12) ـ نسب إقبال المستخدمين الإيرانيين على مختلف تطبيقات التواصل الاجتماعي خلال عام 2015[42].

تطبيق التواصل الاجتماعي	نسبة المستخدمين
Facebook	24.27 %
Twitter	17.69 %
LinkedIn	15.63 %
Google +	11.79 %
Pinterest	6.92 %
You Tube	6.02 %
Stumble Upon	5.86 %
Vimeo	5.12 %
Other	6.7 %

ويبدو واضحاً أن هناك شريحة واسعة تستخدم هذه التطبيقات التي قد تكلف أصحابها احكاماً بالسجن، أو عقوبات أخرى رادعة. واقد أسهم إقبال رأس الهرم الحكومي على خدمات التواصل الاجتماعي المحظورة، مثل الدكتور محمد جواد ظريف ـ وزير الخارجية، والدكتور حسن روحاني ـ رئيس الجمهورية لهذه الخدمات، ونشرهم للكثير من آرائهم على جدران مواقعها، أو اطلاق تغريداتهم المستمرة على إضفاء بصمة الأمل لدى الطبقة المثقفة بإيران، وشريحة الناشطين بوجود فرصة قريبة لرفع عملية الحظر والعودة الى حالة الانفتاح على هذا الفضاء الرحيب في وقت قريب، فمل يهجروا الفضاء التواصلي المحظور لغاية هذا التاريخ.

3 . 3 . 1 . شبكة التواصل الاجتماعي *Facebook* بنسختيها العولمية والايرانية:

رغم أن السلطات الإيرانية قد حظرت موقع شبكة التواصل الاجتماعي *Facebook* وعدّت استخدامه جريمة يحاسب عليها القانون[43]، فلا زال المواطن الإيراني مستمراً بالمشاركة في هذا الموقع في أنشطة الاتصال والتواصل مع الغير، ومن خلال توظيف مختلف آليات تجاوز عقبة الحظر، سواء عن طريق شبكات الشبكات الخاصة الافتراضية *VPN* او أي

42 . الموقع: *https://www.statsmonkey.com/table/21607-iran-desktop-social-network-usage-statistics-2015.*

43 . أصدرت عام 2014 عدة أحكام بالسجن تراوحت بين خمس الى سبع سنوات بحق كل من: مسعود سعيد طالبي، فريد اكرمبور، فاريبوز كاردار فرد، مسعود غاسيمخاني، امير جولاستاني، ومهدي ريشاهري بسبب إصدارهم منشورات على صفحاتهم في موقع *Facebook*.

يمكن مراجعة المقال: *http://www.iranhumanrights.org/2015/04/final-verdict-facebook-users/*

آلية تتوفر في فضاء الانترنيت لدعم أنشطة قرصنة عمليات الحجب والحظر التي تمارس في إيران أو غيرها من الدول التي صنفت بوصفها دول معادية لخدمات التواصل الاجتماعي على الانترنيت[44].

في البداية، ومع غياب عمليات الحظر، وجد هذا الموقع سوقاً رائجة في إيران فسجّل فيه طيف واسع من المستخدمين التقليديين، حتى بدأ بالتحول الى ساحة المتغير السياسي الإيراني، فأضحى بيئة خصبة تستوطن فيها خطابات المعارضة، وتتوطد من خلال خدماته السيبرانية الصلات بين أعضائها، والمجاميع المنبثقة عنها داخل حدود إيران وخارجها.

ويبدو واضحاً من تتبع مجاميع المعارضة الإيرانية المنبثة بكثافة على موقع *Facebook* أن حضورها قد اتسم بما يأتي: رغم حظر مجهزي خدمة الانترنيت لهذه الخدمة في إيران لمدة بضعة سنوات، فقد عمدت الحكومة الى فتح الموقع في شهر كانون الثاني عام 2009، بيد أنها قد عاودت الكرّة بإغلاقه بعد أن وجدت أن أنصار موسوي قد وظفوا هذا الموقع لشد أزر حركته المعارضة فتجاوز عددهم على 5000 مؤازر، وبقي الموقع مغلقاً في الفترة التي تلت الانتخابات.

ولا زال الإيرانيون يوظفوا تقنيات القرصنة السيبرانية للدخول الى هذا الموقع، وترسيخ مناصرتهم للمعارضة وتوثيق الاتصالات والتنسيق بين مجاميعها المختلفة. فعلى سبيل المثال هناك أكثر من 110 آلاف مؤازر لصفحة موسوي باللغتين الفارسية والإنجليزية حول العالم، كما أن موسوي ذاته يقوم بإرسال عدة رسائل كل بضعة ساعات يومياً.

بروز دعم عولمي للمعارضة الإيرانية على صفحات هذا الموقع، يمكن ملاحظته عبر المجاميع المتنامية التي تدعم النزعة التحررية لدى المعارضة، وتحاول نشر خطابها الى مساحة أكبر من المستخدمين. فعلى سبيل المثال ظهرت مجموعة جديدة أطلقت على نفسها " 100 مليون من أعضاء *Facebook* لدعم الديمقراطية في إيران" والتي أنشأها مواطن من مدينة نيويورك، ووصل أعداد المشاركين بالمجموعة أكثر من 208 آلاف مؤازر.

بصورة عامة لا تتوفر إحصائية دقيقة عن عدد مستخدمي هذا الموقع، بسبب وصولهم الى منصة التطبيق عبر قنوات افتراضية تخفي معالم البصمة السيبرانية للمستخدم، وتمنحه حضوراً افتراضياً في فضاء التواصل الاجتماعي. كذلك فإن معظم المستخدمين يستخدمون هوية رقمية مستعارة Avatar لا تمت بصلة حقيقية بهويتهم الحقيقية. لذا فإن كل الاحصائيات التي تتحدث عن حضور المواطن الإيراني في هذا الفضاء التواصلي لن تكون قريبة للواقع.

وقد توفرت بين أيدينا إحصائية قامت بإعدادها الناشطة الإيرانية جميلة كنولاس[45] والتي اكدت فيها أن نسبة مستخدمي هذا الموقع تناهز 58% من مستخدمي الانترنيت (من حملة الشهادات الجامعية والناشطين من المثقفين) بالبلاد، والذين يفضلون استخدام الشبكات الخاصة الافتراضية للوصول خلسة الى صفحاتهم الشخصية والتواصل مع أقاربهم وأصدقائهم بعيداً عن نظم الحجب والحظر الإيرانية.

وأظهرت المسوحات التي قام أعضاء فريق برنامج الوسائط بإيران بمركز دراسات الاتصالات العولمية في جامعة بنسلفانيا بالولايات المتحدة الأمريكية، وشملت شريحة واسعة من مستخدمي موقع شبكة التواصل الاجتماعي *Facebook* في مدينة طهران الحقائق التالية عن استخدام هذا الموقع التواصلي في مدينة طهران بصورة خاصة، وإيران بصورة عامة (*IMP,2014*):

[44] . تشترك تسع دول أخرى مع إيران في حظر خدمة الانترنيت هي كل من: كوريا الشمالية، الصين، كوبا، بنغلاديش، مصر، سوريا، موريتيوس، باكستان، وفيتنام.

[45] . راجع الدراسة على الرابط:

http://thenextweb.com/me/2012/11/08/iranian-online-research-panel-releases-its-latest-study-into-attitudes-and-behaviours-online-inside-iran./

- ✓ يستخدم غالبية مستخدمي موقع Facebook الحواسب الشخصية (بواقع 97 %) بوصفه الأداة الأكثر أمناً لتسللهم الى هذا الموقع الأثير على نفوسهم.
- ✓ يتواصل 92 % من مستخدمي هذا الموقع التواصلي وهم بيوتهم بعيداً عن أنظار الرقيب.
- ✓ تعد الشبكات الخاصة الافتراضية الوسيلة المفضلة للمستخدمين (يستخدمها حوالي 78% من عموم المستخدمين) للتسلل من الفجوات المقيمة في نظم الحجب والحظر السيبراني التي تسخرها الحكومة لحظر هذه الخدمة التواصلية.
- ✓ يشيع استخدام الشبكات الخاصة الافتراضية بين مختلف الفئات العمرية التي تتواصل من خلال موقع *Facebook* (الفئات العمرية التي تقل عن 25 سنة بنسبة 72 %، الفئة العمرية 25-29 سنة بنسبة 82 %، الفئة العمرية 30-39 سنة بنسبة 74 %، اما الفئة التي تتجاوز أعمارها 40 سنة فتصل نسبة استخدامهم لهذه الأداة الى 98 %).
- ✓ يتكرر مراجعة صفحات المشتركين بهذه الخدمة بمستويات متعددة، فيراجع 59% من المشتركين صفحاتهم أكثر من مرة يومياً، بينما يراجعها 27 % من المشتركين مرة يومياً، بينما لا يراجعها بصورة مستمرة 2 % من المشتركين.
- ✓ يقضي المشتركون اوقاتاً متباينة في صفحاتهم على هذا الموقع، فهناك حوالي 32 % من المستخدمين ممن يقضون أكثر من 10 ساعات يومياً، بين يقضي 19 % من المستخدمين مدة تتراوح بين 5-10 ساعات يومياً، ويقضي 15 % منهم بين 3-5 ساعات يومياً. وهناك 17 % ممن لا يستغرقون في صفحاتهم أكثر من ساعة واحدة يومياً.
- ✓ يعد نشاط التواصل مع الأهل والصدقاء من أكثر الأنشطة التواصلية التي يفضلها 60 % من مستخدمي هذا الموقع، بينما يستخدم 16 % منهم الموقع لتعميق معرفتهم بكثير من المسائل التي تخص حياتهم اليومية، وحوالي 11% للاستمتاع.
- ✓ ويبدو أن هناك نسبة ضئيلة من المستخدمين الذين يتواصلون حول المسائل التي تخص الأمور الدينية. فيلاحظ عدم شيوع هذه الممارسة لدى الذين تتجاوز أعمارهم 40 سنة، بينما تصل النسبة الى 2 % لدى الذين تتراوح أعمارهم بين 30-39 سنة، و8% لدى الذين تتراوح أعمارهم بين 25-29 سنة، وترتفع النسبة الى 18 % لدى الذين تقل أعمارهم عن 25 سنة في مؤشر يؤكد استخدام شباب الثورة الإسلامية، وطلبة الحوزات العلمية لهذه الخدمة للترويج عن خطاطتهم العقدية، رغم النداءات المتكررة من قبل المرجعيات لهذه الشريحة باتقاء فتنة هذه الشبكة التواصلية.

ورغم الحظر الذي تمارسه المؤسسات الأمنية على هذا الموقع فقد ترعرعت الكثير من صفحات التواصل الإيرانية من داخل إيران وخارجه وبمختلف القطاعات لتلبي حاجات الناطقين باللغة الفارسية، ممن يديمون التسلل عبر القنوات الخفية للتواصل التي توفرها الشبكات الخاصة الافتراضية، وغيرها من أدوات التسلل السيبراني ـ أنظر الجدول (2 - 13).

الجدول (2 - 13) ـ تحليل المجالات العامة لحضور الموطن الإيراني في موقع *Facebook* .

المجال	المرتبة الأولى		المرتبة الثانية		المرتبة الثالثة	
	الموقع	عديد الاعجاب	الموقع	عديد الاعجاب	الموقع	عديد الاعجاب
العلامات التجارية.	Media world	1,024,164	BeroozResani	607,442	Beachnews.com	316,829
المشاهير.	Ebi	2,469,962	Arash	2,445,192	Shadmehr	2,299,661
الجماعات.	Persian Music	1,155,831	Gokfa	945,910	MyStealthy Freedom	884,579
التسلية.	ShowderClub	446,401	X-Faktor	429,906	Sziget Festival	353,144
وسائل الاعلام.	Alam News Channel	3,587,347	Mauto TV	2,621,124	BBC Persian	2,608,519
الأمكنة.	Bam Tehran	357,955	شيراز ما	96,618	Meet Iran	50,542
المجتمع.	Javad Zarif	935,409	USADarFarsi	551,475	Reza Bahlavi	524,654
الرياضة.	Perspolis	373,387	EsteghlalFC	241,229	FC Perspolis	121,500

المصدر: *http://www.socialbakers.com/statistics/facebook.*

بالمقابل فإن قيام السلطات الإيرانية بتوفير منصتي *Facenama + Cloob* بوصفهما أداة محلية بديلة للتواصل الاجتماعي الآمن للمواطن الإيراني، ودون وجود عمليات حظر على المستخدمين، قد أجبر شريحة كبيرة من مستخدمي الانترنيت في إيران باستخدام هاتين الاداتين للتواصل مع الأهل والأصدقاء، ونشر الأفكار، والمشاركة، للتعويض عن القطيعة التي فرضت عليهم موقع *Facebook* الأثير على قلوبهم.

وقد بدأت هذه المواقع تحتل مكانة متقدمة بين المواقع التي يفضلها مستخدمو الانترنيت بإيران، فبحسب احصائيات موقع *Alexa* لتقييم مرتبة المواقع الالكترونية على الانترنيت، خلال النصف الثاني من عام 2015، احتل موقع *Facenama* الموقع المرتبة 11 ضمن المواقع الإيرانية، وبلغت نسبة زائريه من داخل إيران حوالي 85.8 %، بينما زاره إيرانيون مقيمين في دول أخرى وبنسب متفاوتة (4.6 % من المستخدمين المقيمين في روسيا، و2.1 % ممن يقيمون في هولندا، 1% ممن يقيمون في البرازيل، وحوالي 0.8% ممن يقيمون بالهند)[46]. أما موقع *Cloob* فقد احتل الموقع المرتبة 35 في قائمة المواقع الإيرانية، وبلغت نسبة زائريه من داخل إيران حوالي 84.18 %، بينما يزوره إيرانيون يقيمون في دول أخرى وبنسب متفاوتة (5.9 % من المستخدمين المقيمين في روسيا، و4.8 % ممن يقيمون في هولندا، 1.41% ممن يقيمون في البرازيل، وحوالي 1% ممن يقيمون الولايات المتحدة)[47].

وتظهر المقارنة بين الموقع الأم الذي حاول الإيرانيون محاكاته، وموقعيهم البديلين، أن هناك بوناً شاسعاً على صعيد عديد المستخدمين، وحجم العوائد المتحققة، بسبب انحصار الموقعين داخل حدود إيران، بينما انفتح الموقع الأم على عموم الفضاء العولمي للانترنيت ـ أنظر الجدول (2 - 14).

[46] . يمكن مراجعة المزيد من التفاصيل على الصفحة: *http://www.alexa.com/siteinfo/facenama.com.*

[47] . يمكن مراجعة المزيد من التفاصيل على الصفحة: *http://www.alexa.com/siteinfo/cloob.com*



الجدول (2 - 14) ـ مقارنة بين موقع *Facebook* والموقعين البديلين الإيرانيين *Facenama + Cloob*.

الوصف	موقع Facebook	المواقع الإيرانية البديلة	
		Facenama	*Cloob*
المرتبة وفق تبويب Alexa الدولي.	2	796	1,754
المرتبة وفق تبويب شركة Google.	9/10	2/10	6/10
الريع اليومي المتحقق، دولار.	5,491,891	75,298	24,773
الريع الشهري المتحقق، دولار.	167,155,874	2,291,289	754,012
الريع السنوي المتحقق، دولار.	2,004,540,353	27,483,710	9,042,149
عدد الزوار، يومياً.	523,037,274	11,674,083	3,840,777
عدد الزوار، شهرياً.	15,919,607,001	355,322,312	116,901,153
عدد الزوار، سنوياً.	190,908,605,010	4,261,040,295	1,401,883,605
زمن تحميل الصفحة، ثانية.	2.85	2.0	1.31
عدد الارتباطات بالمواقع الأخرى.	7,673,400	9,740	73,479

المصدر: http://w3snoopm.com بتاريخ *27 / 10/ 2015*.

وقد تفوق موقع *Cloob* على موقع *Facenama* على صعيد تبويب شركة *Google* لمرتبة الصفحات، وبزمن تحميل صفحاته، وعدد الارتباطات التشعبية التي يقيمها مع مواقع أخرى. بينما تراجع عنه على صعيد مرتبته العولمية وفق موقع *Alexa*، وحجم الريع المتحقق عن أنشطته، وعدد الزوار الذي قارب 12 مليون زائر يومياً.

ويمكن أن يعزى تطور هذه المواقع، نتيجة لإقبال شريحة واسعة من المستخدمين ممن لا يمتلكون مهارات معلوماتية توفر لهم فرصة تجاوز عقبة الحظر، او أولئك الذين لا يميلون ممارسة أنشطة تواصلية تتعارض مع سياسة الحكومة الإيرانية، وتوجيهات المرجعية الدينية، وبدأت أعداد زوارها تتزايد يوماً بعد يوم حتى جاوز عدد زوار هذين الموقعين بضعة عشر مليوناً يومياً، من داخل حدود إيران وخارجها.

3 . 3 . 2 . الإيرانيون ومنصة التغريدات السيرانية *Twitter*:

يلتحق تطبيق *Twitter* بمنصات شبكات التواصل الاجتماعي، ويطلق عليه في كثير من الأحيان، "التدوين المصغّر *Micro Blogging*" كونه يجمع بين ممارسة التدوين السيبراني، والتواصل السيبرانين بعبارات لا يتجاوز عدد حروفها 140 حرفاً. ويتميز هذا التطبيق بعدم حاجته الى التوطن في موقع ويب، ويستطيع المغرّد إرسال تغريدته مباشرة من هاتفه المحمول، أو حاسب اللوحي أو المحمول، دون الحاجة الى المرور بموقع الويب الرئيسي الذي يستضيف هذه الخدمة التواصلية.

وقد وجد موقع التغريد الالكتروني *Twitter* إقبالاً كبيراً بين مستخدمي الانترنيت في إيران، بعد أن ألفوا التعامل مع المدوّنات الالكترونية، كما أنه قد وفّر لهم فرصة بنشر الكثير من التغريدات القصيرة والمتنوعة، وبحرية اكبر من ممارسة التدوين الذي يتطلب جهداً ومتابعة أكبر (*CIMA, 2009*).

ولكثرة شغف الإيرانيين بنشر تغريداتهم السيبرانية، تبوأت إيران، عام 2012، المرتبة التاسعة على صعيد أكثر عشرة دول العالم التي يستوطن فيها المغردين بين المواطنين السيبرانيين الذين يستخدمون الانترنيت (0.88 % مغرّد من المجموع الكلي لمستخدمي الانترنيت بينما تحتل الولايات المتحدة المرتبة الأولى وبنسبة بلغت 50.99 %)[48].

وقد تنوعت مجالات التغريد السيبراني لدى الإيرانيين، وتباينت موضوعاته، فشملت مساحة واسعة من مفردات حياتهم، ومعاناتهم اليومية ـ أنظر الجدول (2 - 15).

الجدول (2 - 15) ـ تحليل المجالات العامة لحضور الموطن الإيراني في موقع *Twitter* عام 2015.

المجال	المرتبة الأولى		المرتبة الثانية		المرتبة الثالثة	
	الحساب	عديد المتابعين	الحساب	عديد المتابعين	الحساب	عديد المتابعين
العلامات التجارية.	Carterer	22,731	MTN Irancell	12,432	Lighter Life	5,580
المشاهير.	Sumi Yusuf	482,953	Jazmin Music	200,704	Payam Zamani	190,672
الجماعات.	@alamNews	257,765	Saad Al-Sharifi	216,594	دراسات	92,567
التسلية.	Avarg Music	7	…	…	…	…
وسائل الاعلام.	VOA Farsi	263,816	Radio Farada	161,284	روزنامه	102,566
الأمكنة.	…	…	…	….	…	…
المجتمع.	Hassan Rouhani	388,213	Javad Zarif	335,520	دكتر حسن روحاني	183,952
الرياضة.	Hamed Haddadi	618	…	….	…	…

المصدر: ***http://www.socialbakers.com/statistics/Twitter.***

ونتيجة لعملية الحظر التي مارستها الحكومة الإيرانية على هذا الموقع، وعلى التوازي مع موقع *Facebook* يلاحظ تراجع عدد المتابعين لمجالات التغريد السيبراني، حتى في المراتب الأولى.

ولم تغب هذه الخدمة التواصلية عن بال المعارضة الإيرانية، وبمختلف تياراتها وتوجهاتها، فسعت الى توظيف فضائه المفتوح، وفرص تجاوزه لعقبة الحظر الذي تفرضه الحكومة في بث خطابها المناهض للحكومة، وثقافة الثورة الإسلامية.

فاستخدم هذا الموقع بوصفه فضاء معلوماتي مواز للواقع الذي عاشته المعارضة الإيرانية خلال عام 2009، واستثمرته لنشر حجم كبير من المعلومات التي حظرت الحكومة نشرها على وسائل الإعلام، فاستنفرت الرأي العام، ووفرت بيئة إخبارية تجاوزت عقبة الرقابة الصارمة التي مارستها السلطة على المعارضة والشعب.

لقد استخدمت المعارضة الإيرانية التغريدات السيبرانية ووظفت قدراتها الاتصالية لخدمة خطابها السياسي من خلال :(*CIMA, 2009*)

48 . راجع الموقع: http://www.beevolve.com/twitter-statistics/.



- إقامة بيئة اتصالية آمنة لاستكمال تشكيل تفاصيل الحدث السياسي الدائر على أرض المواجهة مع النظام الإيراني وبثها داخل حدود إيران وخارجها بأشكال متعددة تظهر بجلاء ما يمارسه النظام على الأرض في مواجهاته الدائمة معها.
- تجاوز عقبة المراقبة الصارمة التي تمارسها السلطات الأمنية على وسائل الإعلام المنتشرة على مواقع الانترنيت، أو الوسائط التقليدية، لأن عمليات الكف التي تمارسها نظم حجب موقع التغريدات لم تفلح في منع إرسال تغريداتهم بصورة مباشرة من الهواتف المحمولة الى الموقع عبر المنظومة الهاتفية، فتنتشر أخبار المعارضة وخططها على مساحة واسعة.
- استثمار قدرات الموقع (على نقل الوسائط المتعددة) في نشر وثائق مصورة الى المنظمات الانسانية، والرأي العام العالمي، والى من يعنون بالدفاع عن حقوق الإنسان عبر صور وأفلام توثق حقيقة ما يحصل على أرض إيران، مع إمكانية توسيع رقعة انتشار الخبر بعد ان يعاد نقله آلياً الى مواقع أخرى تمتد على رقعة مواقع الانترنيت غير المتناهية.

وأظهرت الدراسة التي قامت بها فريق مشروع بيئة الويب *WEB Ecology Project* حول أنماط التغريدات السيبرانية التي سادت موقع *Twitter* حجم النشاط الذي مارسه هذا الموقع على صعيد الانتخابات الرئاسية بإيران خلال عام 2009. فقد بلغ عدد التغريدات السيبرانية خلال حملة الانتخابات الرئاسية التي امتدت بين 7-26 حزيران من عام 2009 قد بلغت حوالي 2,024,166 تغريدة، شارك بها أكثر من 480 ألف مستخدم إيراني (*WEP,2009*).

وقد توزعت مفردات هذه التغريدات على عموم الفضاء السياسي للعملية الانتخابية ـ أنظر الجدول (2 - 16)، فكانت مفردة إيران، رمز المواطنة والانتماء، بالمرتبة الأولى، ثم مفردة الانتخابات بوصفها الحدث الأهم بالمرتبة الثانية، ثم طهران، التي كانت نقطة انطلاق التيارات المعارضة، وحسين موسوي وخطابه المعارض، والباسيج وممارساته القمعية ضد الفئات المعارضة، وأحمدي نجاد، فالخميني، وأخيراً رفسنجاني الذي خفت بريق سلطته عن الساحة السياسية للانتخابات الإيرانية.

الجدول (2 - 16) ـ موضوعات التغريدات السيبرانية التي صاحبت أحداث الانتخابات الرئاسية الإيرانية.

المفردة	عدد التغريدات
إيران.	903,193
الانتخابات الإيرانية.	867,401
طهران.	85,019
حسين موسوي.	16,970
الباسيج.	3,295
احمدي نجاد.	1,765
الخميني.	1,409
هاشمي رفسنجاني.	77

لقد أدركت وزارة الخارجية الأمريكية الدور المهم الذي يمكن أن يمارسه هذا الموقع على الحدث السياسي في إيران فعمدت الى إقناع إدارة الموقع بالكف عن إيقاف الموقع لإجراء الصيانة الدورية لمحتوى الموقع خلال الفترة التي

احتدمت مواجهات المعارضة الإيرانية مع النظام بعيد إعلان نتائج انتخابات الرئاسة (*Parteni,2009*) لتوفير فرصة ثمينة للمعارضة الإيرانية في بسط خطابها السياسي المعارض عبر أدوات هذه الخدمة.

ونود أن نبين أنه رغم الحظر الحكومي الصارم على ممارسة التغريدات السيبرانية، فإن الكثير من المسؤولين الإيرانيين مثل: محمد جواد ظريف (وزير الخارجية الحالي ـ بلغ عدد متابعي تغريداته أكثر من 350 ألف متابع)، وحسن روحاني (رئيس الجمهورية الإيرانية ـ بلغ عدد متابعي تغريداته أكثر من 500 ألف متابع)، وكذلك الحال بالنسبة للمرشد الأعلى للثورة الإسلامية، الذين لا يزالون يمارسون عملية التغريد السيبراني المفتوح لهم، دون غيرهم، وحول مواضيع سياسية وعقدية متنوعة[49].

3 .3 . 3 . الإيرانيون وبوابات أخرى للتواصل الاجتماعي:

كان موقع *You Tube* (لمشاركة الملفات الفيديوية) متاحاً للمستخدمين الإيرانيين، دون وجود أي عملية حظر، بيد أن الدعوات المتكررة من المرجعيات الدينية حول المحتوى غير الملتزم بقيم الإسلام وثقافة الثورة الإسلامية قد وجه أنظار الحكومة الى التفكير بحظر الموقع.

لم تخل ساحة هذا الموقع من أنشطة المعارضة الإيرانية، والتي حرصت على أن تودع فيه كل الأحداث التي يعجز الصحفيون عن الحديث عنها في الصحف اليومية، وما تريد أن تفضحه المعارضة عن ممارسات النظام القمعية.

وللوقوف الى ما يحفل به هذا الموقع عن الاحتجاجات المستمرة للمعارضة الإيرانية قمنا بالتنقير عن المقاطع الفيديوية الموجودة على هذا الموقع يوم 2010/1/9 فظهرت لنا الإحصائيات التي أودعنا بياناتها في الجدول (2 - 17).

الجدول (2 - 17) ـ عناوين المقاطع المودعة في موقع *YouTube* حول المتغير السياسي الإيراني.

الموضوع	عدد المقاطع الفيديوية
أحمدي نجاد.	34,900
حسين موسوي.	14,500
مهدي كروبي.	2,400
محمد خاتمي.	3,660
الانتخابات الإيرانية.	85,300
احتجاجات المعارضة الإيرانية	105,973
الاحتجاجات اليومية.	74,100
احتجاجات عاشوراء.	3,160
إطلاق النار على المحتجين.	419
هجوم الشرطة على المحتجين.	324
حوادث قتل المحتجين.	2,870
المرأة الإيرانية في المواجهة.	25,100
الانتخابات الإيرانية.	85,300

[49]. بحسب ما نقلته صحيفة *The Huffington Post* البريطانية في عددها الصادر في 8 سبتمبر 2015 أن المرشد الأعلى للثورة الإسلامية في إيران آية الله علي خامنئي قد غرّد على موقعه أن إسرائيل ستزول حتماً خلال السنوات 25 القادمة.
راجع موقع الجريدة: *http://www.huffingtonpost.co.uk/uk*.

وقد وفرت الإدارة الحكومية الإيرانية موقعاً إيرانياً بديلاً هو موقع *Aparat* دخل للعمل في بداية عام 2011 للتعويض عن الفراغ الذي نشب عن حجب موقع *You Tube*. احتل الموقع الجديد (بحسب تصنيف موقع *Alexa* العولمي) المرتبة 557، وتسنم محتوى صفحاته مرتبة 10/4 بحسب تبويب *Google Page Rank*. وقد بلغ عدد زواره في النصف الثاني من عام 2015 حوالي 1,835,449 زائر يومياً، اما عدد المشاهدات اليومية لمحتواه فقد قاربت 15 مليون مشاهدة يومياً[50].

أما موقع *Instagram* للمشاركة بالصور فقد شهد إقبالاً، شأن غيره من مواقع التواصل الاجتماعي في إيران، وبدأ المستخدمين بالمشاركة بصورهم من خلاله. وقد بلغ عدد الإيرانيون الذين يستخدمون هذا الموقع أكثر من 7.5 مليون مستخدم تتراوح أعمارهم بين 15-30 سنة.

بيد أن هذا الموقع لم يسلم من انتقادات حاملي راية ثقافة الثورة الإسلامية، والمرجعيات الدينية فتعرض للحجب، مما اضطر الحكومة الإيرانية الى إنشاء منصة برمجية بديلة أطلق عليها *Lenzor* لدعم عمليات مشاركة الإيرانيين بصورهم الشخصية في بيئة معلوماتية آمنة (*SMO,2014,c*).

احتل الموقع مرتبة متراجعة ضمن التبويب العولمي لموقع *Alexa* فاستقر في المرتبة 30,138، كذلك تراجع مستوى محتوى صفحاته فلم يظفر الا بالمرتبة 10/2 بحسب تصنيف *Google Page Rank*. وبلغ عدد زوار صفحات الموقع حوالي 32 ألف زائر يومياً، بينما عدد المشاهدات لمحتواه الصوري حوالي 192 ألف مشاهدة يومياً ـ خلال النصف الثاني من عام 2015[51].

3 . 4 . البصمة السيبرانية الإيرانية في موسوعة *Wikipedia*:

بزغت فكرة موسوعة ويكيبيديا في الربع الأول من عام 2000 عندما أرسل *Jimmy Wales* (أحد مؤسسي موسوعة ويكيبيديا) رسالته الأولى الى قائمة موسوعة *Nupedia*[52] البريدية "حلمي أن تتوفر في يوم من الأيام موسوعة وبثمن لا يتجاوز كلفة طباعتها في المدارس المنتشرة بجميع بقاع الأرض، وبضمنها بلدان العالم الثالث التي لا تمتلك القدرة على إتاحة فرصة الوصول الى خدمة الانترنيت خلال الأعوام المقبلة"(*Reagle,2010*).

وقد بدأت دلالة المصطلح بالنمو وتعمق حضوره فأضحى يطلق على مجموعة من المواقع التي يتألف محتواها السيبراني من مجموعة النصوص التي يدونها مجموعة من المؤلفين بقصد إنشاء خطاب معرفي في حقل من الحقول. ورغم أن هناك كثير من النقاط المشتركة بين فضاء ويكي وفضاء المدونات على صعيد البنية المنطقية، إلا أن بيئة ويكي تتميز بكونها منفتحة كلياً أمام الآخر على صعيد إعادة إنتاج المحتوى المطروح، أو تعديله، بواسطة أي مستخدم، في حين تقتصر هذه العمليات على صاحب المدونة في الفضاء السيبراني للمدونات(*Lih,2009*).

لقد أسهمت موسوعة ويكيبيديا بترسيخ مفهوم جديد ارتبط بثقافة رقمية مستحدثة باتت تعرف بالثقافة التعاونية *Collaborative Culture* التي لم تعد حكراً على شريحة من المجتمع بل أضحت نتاجاً معرفياً يتعاون على توليد مادته، وإثرائها مجموعة من المستخدمين، أثناء حضورهم في بيئة الانترنيت.

وقد ولدت النسخة الفارسية من هذه الموسوعة في نهاية عام 2003 (ویکی‌پدیا، دانشنامهٔ آزاد) فهرع المدونون الإيرانيون، والمثقفون، وشريحة واسعة من أهل العلم والمعرفة بكتابة الكثير من المقالات بلغتهم الأم، فتوسعت مادة

---

[50] . بحسب بيانات الموقع: http://www.iwebsiteworth.com/www/aparat.com

[51] . بحسب بيانات الموقع: http://www.iwebsiteworth.com/www/Lenzor.com

[52] . موسوعة باللغة الإنجليزية أنشأها جيمي والاس عام 2000 استوطنت موقعاً من مواقع الويب، استمر حضورها السيبراني لمدة ثلاث سنوات فتوقفت عام 2003.

المحتوى، وتناسلت المقالات حتى بلغ عددها في نهاية عام 2004 أكثر من ألف مقال، واستمرت عملية البناء الموسوعي لمادة الموسوعة حتى بلغ عديد مقالاتها في منتصف عام 2012 حوالي 200 ألف مقال (*Wikipedia,2015*).

ولم يحل شهر يناير من عام 2013 حتى بلغ عدد المقالات الملتحقة بفضاء الموسوعة السيبرانية الإيرانية حوالي 50 ألف مقال خلال شهر واحد، وعند منتصف شهر فبراير من عام 2013 بلغ عدد المقالات الكلية للموسوعة السيبرانية الفارسية الإيرانية أكثر من 300 ألف مقال ـ أنظر الجدول (2 - 18).

الجدول (2 - 18) ـ نمو عدد مقالات الموسوعة السيبرانية الإيرانية خلال السنوات 2003-2014.

السنة	عدد المقالات
2003	البداية
2008	50,000
2010	100,000
2012	200,000
2013	300,000
2014	400,000

المصدر: *Wikipedia,2015*.

واستمر الإيرانيون في صناعة محتوى رقمي مميز انصبغ بلغتهم الفارسية لترسيخ حضورهم السيبراني قبالة الحضور الذي يمارسه بقية المستخدمين الذين يبذلون ما بوسعهم لمغالبة التيار الهادر الذي تمارسه اللغة الإنجليزية في هيمنتها شبه المطلقة على المحتوى السيبراني المطروح على صفحات الويب والذي بلغ في الربع الأول من عام 2015 حوالي %55.5.

ولم يقف الحصار التقني والاقتصادي المفروض على إيران خلال السنوات الماضية، مع تباطؤ سرعة الانترنيت، وتضييق حزمة خدماتها بسبب الرقابة الصارمة التي تنتهجها الحكومة والمؤسسة الدينية على شبكة الانترنيت، إلا أن الإصرار الذي تتسم به الهوية الإيرانية لم تمنع بل حفّزت المستخدم الإيراني على إنتاج حجم أكبر من المحتوى السيبراني، وبمجالات متعددة، بحيث نجحت إيران بمفردها في إنتاج محتوى، نافس رغم ضآلته المحتوى السيبراني العربي (شكل المحتوى السيبراني المطروح على مواقع الويب والناطق باللغة الفارسية حوالي 0.9 % من المحتوى العولمي، بينما بلغ المحتوى الناطق باللغة العربية فقط 0.8 %) من أجل هذا احتلت الموسوعة الناطقة باللغة الفارسية المرتبة 18 بين جميع موسوعات *Wikipedia* الناطقة بمختلف لغات العالم، متفوقة على تلك المدونة باللغة العربية والتي احتلت المرتبة 21 (*Wikipedia,2015*) ـ أنظر الجدول (2 - 19).

الجدول (2 - 19) ـ موقع موسوعة ويكيبيديا اللغة الفارسية بين بقية اللغات العالمية.

المرتبة	اللغة	عدد المقالات	التحرير	عدد المستخدمين	المستخدمين النشطين[53]	عمق المحتوى[54]
1	الإنجليزية.	37,279,617	791,595,357	26,290,468	124,980	896
2	السويدي	4,664,499	30,490,034	457,403	2,599	11
3	الألمانية.	5,275,228	151,607,409	2,257,524	18,466	97
5	الفرنسية.	7,699,992	121,224,243	2,330,303	14,873	207
7	الروسية.	4,526,891	85,829,447	1,753,483	9,834	129
18	الفارسية.	3,106,121	20,760,912	529,087	2,850	211
21	العربية	2,383,125	19,732,805	1,069,386	3,459	226
30	التركية.	1,370,833	17,039,628	790,904	3,239	242
39	اليهودية.	747,465	18,425,895	282,851	1,986	252

المصدر: *Wikipedia,2015, On 26 September*.

وقد اتسم المحتوى المعرفي المطروح في الموسوعة الفارسية، بكثرة ارتباطاته التشعبية، الأمر الذي جعل الموسوعة تحتل المرتبة الخامسة عالمياً على صعيد عمق المحتوى بين بقية موسوعات *Wikipedia* السيبرانية ـ راجع الجدول السابق.

وكجزء من ابتكارات المعارضة الإيرانية في توظيف تطبيقات الالفضاء السيبرانيي لنشر خطابها المعارض، فقد استخدمت ثلّة من المدونين المعارضين بيئة الموسوعة السيبرانية في استضافة مجموعة كبيرة من المقالات، لم تلبث أن تطورت الى صحيفة مستقلة استوطنت فضاء الموسوعة وأطلق عليها "الانتخابات الرئاسية الإيرانية لعام 2009" فتكاثرت النصوص التي تدخلها المعارضة على محتوى الصفحة، حتى بلغت التعديلات التي تمت على محتوى هذه الصفحة في يوم 14 حزيران "يوم احتجاج المعارضة" أكثر من 300 تعديل، حيث باشر المعارضون بتعديل وصفهم للحدث خلال دقائق من الحدث. وقد تحول هذا الموقع، شيئاً فشيئاً، من موقع موسوعي الى موقع إخباري يعجّ بما يدور من مواجهات بين المعارضة والنظام الإيراني (*CIMA,2009*).

ولم يدخل عام 2013 حتى شملت الموسوعة بإجراءات الرقابة والحظر لدرء هذه المخاطر، فبدأت بتقطير مادة المحتوى المطروح الى الموسوعة السيبرانية، حيث حظرت في السنة ذاتها أكثر من 963 مقال، بحجة معارضتها لثقافة الثورة الإسلامية ومرتكزاتها الأخلاقية. ولا زالت عملية الرقابة وتقطير المحتوى مستمرة لضمان عدم تسرب معلومات أو مقالات مناهضة للثورة الإسلامية وخطاطتها الثقافية في فضاء الموسوعة الناطقة باللغة الفارسية.

4 . شبكة الانترنيت الوطنية: الفضاء الايراني البديل:

لم تستمر الهدنة طويلاً، بين حكومة محمود احمدي نجاد وبين فضاء الانترنيت بعد تزايد ضغوط مؤسسة الحرس الثوري الإيراني، وهاجسها الأمني تجاه المحتوى الذي تحفل به من جهة، وأئمة المرجعيات الدينية التي رأت في هذا الفضاء بوابة مشرعة لتناسل فتن الشيطان ومدخلاً الى تقويض منظومة الأخلاق الإسلامية.

[53] . المستخدمين النشطين هم المستخدمين الذين يساهمون في إعداد مادة مقالات الموسوعة، أو تحرير المحتوى المطروح فيها.

[54] . عمق المحتوى لا صلة له بالمحتوى المعرفي لمادة المقالة، وإنما هو معيار حسابي يعتمد على عدد عمليات التحرير التي زاولها المستخدمين على المحتوى، ووفرة الصفحات الداعمة للمقال والتي تؤشر نحو أهمية محتوى المقالة داخل حدود موسوعة ويكيبيديا.



فكانت الخطوة الأولى بإعلان القطيعة على لسان محمد سليماني (وزير الاتصالات في عهد محمود احمدي نجاد) عن رغبة الحكومة الإيرانية بإنشاء شبكة المعلومات الوطنية *The National Information Network* التي سيتم تشكيل فضائها الشبكاتي، وإعداد مادة المحتوى السيبراني المطروح في عقدها السيبرانية بحيث يتوافق مع ثوابت ثقافة الثورة الإسلامية وقيمها، مع السماح لنشر أدوات مراقبة حكومية للمحتوى، وضمان توافقه مع مبادئ السلوك الإسلامي القويم.

في عام 2006، أطلق الوزير على الشبكة الجديدة اسم "الانترنيت الوطنية *National Internet*"، وذكر ان هذه الشبكة الوطنية ستباشر عملها خلال سنتين، وأكد ان الفضاء الجديد سيوفر مناخاً شبكاتياً ستقوم الحكومة بالإشراف على تنظيم عملية الوصول إليه، واستثمار مادة المحتوى السيبراني المطروح في مستودعات مضيفاته المحلية، في ظل بيئة آمنة تحمي المستخدم الإيراني من ممارسات الاختراق والتجسس السيبراني، مع ضمان مشروعية الاستخدام وفق مبادئ الدين الإسلامي الحنيف.

ومما لا شك فيه أن القدرات الإيرانية السيبرانية والتقنية، وفي ظل حصار تقني مفروض على دولة مارقة مثل إيران، لم تكن كافية لدعم عمليات تحويل مقترح مشروع الانترنيت الوطنية من دائرة الخطاب السياسي والإعلامي الى أرض الواقع خلال مدة قصيرة، الأمر الذي حتّم على الحكومة الاستمرار بعمليات الكفّ السيبراني من خلال تضييق سرعة حزم المعلومات المجهزة للمواطنين في الأماكن العامة، ومناطق سكناهم لضمان كفّ محاولات الوصول الى المواقع التي تناهض الحكومة، أو تدعم خطاب الناشطين بنوعيه الإصلاحي أو المناهض.

بيد أن بصمة الحصار وآثارها الاقتصادية والتقنية على إيران، مع حظر شركات المعلومات العملاقة مثل: *Microsoft*، *Apple*، *Oracle* وغيرها من الشركات من التعامل مع مؤسسات الحكومة الإيرانية، والشركات المحلية، قد أجبر المؤسسات السيبرانية الى التوجه نحو طرف ثالث للحصول على النظم والتطبيقات البرمجية، وبدون وجود الدعم الفني الذي يعضد ويطور عمليات الاستخدام المحلي، قد عزز من الضغوط على الحكومة على الصعيدين الاقتصادي والتقني.

وبالوقت ذاته أسهم الدور الذي مارسته المعارضة الإيرانية خلال الانتخابات الرئاسية عام 2009، واشتعال المواجهة بين النظام وشريحة واسعة من الناشطين الذين استثمروا فضاء الانترنيت لنشر خطابهم، وتوحيد صفوفهم، وتصدير أصواتهم، مدعومة بمشاهد صورية وأخرى مرئية من الشارع الإيراني مباشرة، الى باحة الفضاء السيبراني العولمي، في توجيه أنظار حكومة نجاد نحو إعلان القطيعة المؤقتة مع بعض خدمات هذا الفضاء، والتفكير في إيجاد تطبيقات بديلة يمكن أن تمارس دوراً مقارباً يحتوي عواصف الاحتجاج المحتملة عند التوجه نحو قطع الخدمة دفعة واحدة.

لقد أصبحت شبكة الانترنيت الوطنية أمراً محتوماً بالنسبة لحكومة أحمدي نجاد، ولاقت فكرته دعماً من مؤسسة الحرس الثوري ومرجعية الحوزة الشيعية بعد أن تعمّقت القناعة لدى هذه الجهات الثلاث بخطورة الدور المحتمل لفضاء الانترنيت على الصعيد السياسي، والأمني، والثقافي. فالتحق المشروع بقائمة المشاريع الاستراتيجية بالبلاد، وبدأ يتلقى تخصيصات مالية مجزية، مع تحشيد الحكومة للخبراء والتقنيين من أروقة المؤسسات الأكاديمية، والبحثية، ووزارات الدولة، مع التوجه الى الدول التي لديها علاقات جيدة مع إيران، وتتبنى السياسات ذاتها في التعامل مع فضاء الانترنيت: مثل كوريا الشمالية، والصين، لكي تتلقى من خبرائهم المشورة التقنية وتنهل من الخبرة المتراكمة لديهم لتطوير قدراتهم الوطنية.

4 . 1 . معمارية ومكونات شبكة الانترنيت الحلال[55]:

حددت الفقرة 46 من الخطة الخمسية الوطنية لايران، الإطار العام لعمل شبكة المعلومات الوطنية والتي ستعتمد مبدا معمارية الانترنيت المرتكزة الى بروتوكول *IP* والتي ستدعمها مراكز بيانات خاصة، وتتمتع بحصانة أمنية، لا يمكن الكشف عنها، وغير نافذة أمام محاولات التلصص والاختراق السيبراني. وقد أقرّ المجلس الأعلى لالفضاء السيبراني الإيراني *SCC* في اجتماعه الذي عقد في 24 ديسمبر 2014 المخصصات التقنية التي اقترحت ضمن الخطة الوطنية الخمسية، فأضحى مضمون الفقرة تعريفاً لهوية شبكة الانترنيت الوطنية في إيران.

وقد علّقت آمال كبيرة على الشبكة الوطنية، في تجاوز عقبة تباطؤ سرعة الانترنيت العولمية التي أجبرت الإدارة الحكومية على استخدام آليات متنوعة لحظر وحجب المواقع التي لا تتوافق مع الخطاطة الثقافية للثورة الإسلامية، فانعكست آثارها على سرعة الخدمة بشكل ملحوظ.

وقد رسخ هذه الآمال ما ذهب إليه محمود خسروي (أحد المدراء العاملين في شركة *TCI*) عندما أكد في تصريح له، أن سعة حزمة الفيض السيبراني لشبكة الانترنيت الوطنية *SHOMA* سوف تتضاعف بمقدار عشرين ضعفاً عن الفيض الحالي، لتصل الى *4 TBps* في نهاية عام 2016، ثم تقفز قفزة لاحقة لتبلغ *10 TBps* مع نهاية عام 2017 (*SMO,2015,b*).

ومما لا شك فيه أن مشروعاً مثل مشروع شبكة الانترنيت الوطنية في إيران، يعد من المشاريع العملاقة في المنطقة، ويمثل تحدّياً تقنياً بحاجة الى دراسة متأنية، ووفرة حزمة متنوعة من الموارد لضمان اكتماله، واستمراره، لأن دولاً كبرى مثل الصين، وكوريا الشمالية، لم تفلح (لغاية هذا التاريخ) في تحقيق جميع أهداف مشاريعها الوطنية للانفصال عن الفضاء العولمي لشبكة الانترنيت، والاكتفاء بمواردها ومستودعاتها، وتطبيقاتها السيبرانية بمعزل عن الأدوات، والتطبيقات البرمجية، والمنصات السيبرانية التي تنتشر بكثافة خارج حدود فضائهم الوطني.

كما أن المعمارية التي يفرضها مثل هذا المشروع العملاق لن تقتصر على المعمارية الشبكاتية فحسب، بل تتوسع باتجاه توفير مستودعات رقمية لاستضافة الموارد السيبرانية المحلية، وتوفير محركات بحث، ومستعرضات، وخدمات بريد الكتروني، وتطبيقات لمكافحة البرمجيات الضارة والفايروسات، وجدران نارية لكفّ عمليات اختراق المواقع، ومنصات شبكات التواصل الاجتماعي، وبيئات برمجية متكاملة، وتطبيقات تلبي الحاجات المتزايدة لمختلف فئات المستخدمين.

إن حرص الإدارة الحكومية الإيرانية على إيجاد بديل يمكن أن يعوّض المواطن الإيراني عن جزء محدود من فضاء الانترنيت العولمي، ويقلل من حجم الهاجس الأمني الذي باتت تنوء به مؤسسة الحرس الثوري الإيراني، ويطمئن المرجعية الدينية على سلامة الفضاء الجديد من موارد تخالف الشريعة الإسلامية، مع وجود خبرات عملية وتقنية تمتلك دافعاً وحسّاً وطنياً للنهوض بالبلاد، والارتقاء بها الى مستوى الصدارة بين بقية بلدان المنطقة قد حوّل الحلم شيئاً فشيئاً الى واقع ملموس.

ورغم أن عملية التحوّل لا يمكن أن تعد متكاملة، كما أن المشروع لن يبلغ مساحة كافية من مشهد الطموح المنشود، إلا ان من واجب الناقد المنصف أن يوقر جميع العاملين في مفاصل المشروع على صعيد تصنيع المعدات والأدوات الاتصالية، وإنتاج التطبيقات البرمجية، ونظم التشغيل، ومحركات البحث، والمستعرضات، ومنصات شبكات التواصل

[55] . أطلق البعض على شبكة الانترنيت الوطنية في إيران، اصطلاح "الانترنيت الحلال".

الاجتماعي، لأن نجاح جزء من هذا المشروع سيؤكد لنا ثانية ان إيران حكومة وشعباً قادرة على صناعة أدوات ترسّخ حضورها وسطوتها في أكثر من مجال تقني.

4 . 1 . 1 . مراكز البيانات الوطنية:

حرصت الإدارة الحكومية الإيرانية على بناء قاعدة عريضة من مراكز البيانات *Data Centers* ونشرتها في أكثر من محافظة إيرانية، لضمان توفر بنية تحتية متماسكة، ومستودعات رقمية وطنية قادرة على احتواء الفيض السيبراني المسافر في قنوات الاتصالات والمعلومات، ودعم الإدارة الحكومية في سعيها الدائم لاستكمال عملية إنشاء شبكة وطنية للانترنيت.

وكنتيجة للدعم الحكومي، والبدء بعملية التحوّل نحو إنشاء شبكة الانترنيت الوطنية، وتحقيق مستوى مقبول من الحصانة الأمنية لالفضاء السيبراني في إيران، بدأت مراكز البيانات تتكاثر شيئاً فشيئاً من عام 2012. فسارعت الحكومة الى بناء مراكز لاستضافة بياناتها، كما قام القطاع الخاص بإنشاء مراكز للبيانات تدعم عملية تجهيزه لخدمة الانترنيت في عموم البلاد.

ولغرض جذب مواقع الويب من مضيفاتها المستوطنة في العالم الغربي، عمدت الإدارات السيبرانية لمراكز البيانات الى تطوير البنية التحتية لمراكزها، وتوظيف أدوات ترفع من مستويات الموثوقية بحيث تتعمق ثقة المؤسسات الإيرانية والمواطنين بمراكز البيانات الوطنية، وتشجعهم على الانتقال إليها (*Rahmani,2013*).

بالمقابل لا زالت الكثير من مواقع الويب ومنصات التدوين تلجأ الى المضيفات الغربية نتيجة للهاجس الأمني الذي يقلق المستخدم الإيراني من الرقابة المشدّدة التي تمارسها مراكز البيانات نتيجة للضغط الذي تمارسه الإدارة الحكومية على الشركات الإيرانية المضيفة.

وتعد شركة *Pars Iran* من الشركات السيبرانية والاتصالية الرائدة التي تمتلك أكثر من مركز بيانات، في طهران، ومحافظات إيرانية أخرى، كما أنها تعد من أكبر شركات المجهزة لخدمة الانترنيت في عموم البلاد (*Wikipedia,2015*).

ولم تتوفر لدينا معلومات دقيقة عن عدد مراكز البيانات التابعة للقطاع الحكومي، والقطاع الخاص في عموم إيران، بيد أن بعض المصادر قد اشارت الى وجود حوالي 13 مركز مملوك للبيانات *Colocation Data Centers* يوجد عشرة مراكز منها في العاصمة طهران، ومركز في مشهد، وآخر في همدان، والأخير في رشت.

وأشار محمود خسروي، المدير التنفيذي لشركة *TCI* الإيرانية الى وجود تحرك جدّي نحو زيادة سعة الخدمة المجهزة لهذه المراكز من 43 GB الى 470 GB لكي يرتقي مستوى الخدمات السيبرانية التي تقدمها هذه المراكز لجميع الجهات المستفيدة في البلاد، وتعزز الثقة بها، فتمهد نحو انتقال الشركات من قطاع الشركات المضيفة الغربية، باتجاه مراكز البيانات المحلية.

4 . 1 . 2 . خدمة البريد الالكتروني الوطني:

إن كثرة الاقبال على استخدام البريد الالكتروني على صعيد المؤسسات الحكومية الإيرانية، وقطاع التجارة والأعمال، وشريحة عريضة من المواطنين في عموم إيران، قد وجه أنظار الإدارة الحكومية نحو دعم مشروع لإنشاء منصة خدمات بريد إلكتروني وطنية، بدلاً من الخدمات المانية التي توفرها شركات تمتلك منصات بريد إلكتروني عولمية مثل: *Yahoo.com*، *Gmail.com*، *Hotmail.com*، *Outlook.com*، وغيرها كثير.

بدأت الدعوة الأولى، لإنشاء هذه الخدمة، عندما قام ريزا تاجيبور، وزير الاتصالات في عهد الرئيس السابق محمود أحمدي نجاد بإرسال مذكرة الى وكيله[56]، والى بنك إيران المركزي مؤكداً على ضرورة استخدام البريد الالكتروني المحلي التزاماً بالفقرة 46 من الخطة التنموية الخمسية، والتي أكدت على ضرورة الاهتمام بمسألة أمن المعلومات وحث المصارف الوطنية على استخدام منصات البريد الالكتروني المحلية والتوقف كلياً عن استخدام منصات البريد الالكتروني الأجنبية.

وبدأت قوائم مضيفات خدمة البريد الالكتروني الإيراني، تتوالد يوماً بعد يوم، وظهرت عناوينها التي التحقت بالرموز مثل: *iran.ir*، *post.ir*، *chmail*.، وأصبحت عملية التسجيل بالبريد الالكتروني الوطني مرتبطة بالبطاقة الشخصية الوطنية *National ID*، ورقم الهاتف، وعنوان السكن، لضمان توفير الخدمة للمواطنين الإيرانيين، ومنع عمليات تسلل الغير الى حظيرة خدمة البريد الالكتروني الإيراني.

لقد أصبحت عنونة البريد الالكتروني في إيران، جزءاً لا يتجزأ من مفردات هويته الشخصية التي تحتفظ الإدارات الأمنية بجميع تفاصيل مفرداتها، وأضحت جميع خطاباته السيبرانية مودعة في المستودعات السيبرانية ومراكز البيانات، حيث تستودع مع تفاصيل أخرى ذات صلة بممارساته الشخصية، أثناء حضوره في الفضاء السيبراني للانترنيت، وأصبح محتواها مفتوحاً امام السلطات الحكومية، تنقّر في مضامينه، كيفما تشاء، ومتى تشاء.

ولا زال الكثير من المواطنين الإيرانيين يعرضون عن استخدام خدمة البريد الالكتروني المحلية، بسبب المخاوف من تلصص الحكومة على مراسلاتهم، من جهة، وأن غياب مفاتيح السلامة عن محتوى البريد (لمنح الحكومة فرص التنقير في المحتوى) قد يجعل بريدهم عرضة لأعمال القرصنة الالكترونية. لذا لا زالت هذه الخدمة شائعة لدى المؤسسات الحكومية، والأمنية، ولدى المراكز البحثية، بينما لم تجد لها رواجاً لدى المستخدمين العاديين.

بالمقابل ما انفكت الجهات المعنية تمارس سلسلة من عمليات الدعوة الممنهجة نحو المواطن الإيراني، بالهجرة من ساحة البريد الالكتروني الذي توفره منصات البريد الالكتروني العولمية، والتوجه نحو بريد الكتروني وطني، ناطق بلسان فارسي، وتستقر مضيفاته داخل حدود إيران، بعيداً عن ممارسات التطفل والتلصص والتجسس التي تمارس من قبل المؤسسات الأمنية والمخابراتية للدول الغربية على محتوى البريد السيبراني ـ العولمي (*Anoosheh,2012*).

4 . 1 . 3 . تأمين طبقة الاتصال بفضاء الانترنيت:

يشيع استخدام تقنية طبقة المقابس الآمنة *Secure Sockets Layer* (*SSL*) لإدامة قناة ارتباط آمنة بين مضيف خدمة الويب وزائر مستعرض الويب، بحيث يسمح بانتقال المعلومات الخاصة بالمستخدم دون السماح بالتنصت، أو العبث بمحتوى البيانات، أو تزوير مادة المحتوى السيبراني لقناة التواصل.

لذا فإن حضور هذه الطبقة الآمنة في مضيف خدمة الانترنيت، يرسّخ لدى المستخدم الثقة بأن جميع البيانات التي يتداولها أثناء حضوره في الفضاء السيبراني، لموقع من مواقع الويب، تنتقل في قناة آمنة، ولا يمكن أن يطلّع عليها إلا إدارة المؤسسة التي تمتلك موقع الويب الذي يتواصل معه المستخدم.

وقد أولت الإدارة السيبرانية لشبكة الانترنيت الإيرانية اهتماماً خاصاً بمسألة إصدار شهادات وطنية لتوظيف ومراقبة طبقة المقابس الآمنة، لضمان أمن حزم البيانات التي تسافر في فضاء الانترنيت الإيرانية، والحفاظ على الخصوصية لمحتوى هذه البيانات، وكف أية عمليات تنصّت، أو عبث بمادة المحتوى السيبراني، أو تزويره (*ICHR,2014*).

---

[56] . في بداية عام 2012.

وعمدت بالوقت ذاته الى حظر طيف واسع من الطبقات الآمنة التي تستخدمها مواقع الويب العملاقة، لضمان قدرتها على التحكّم بقنوات تواصل المستخدمين الإيرانيين مع هذه المواقع (تجاوزت الإدارة الأمنية لشبكة الانترنيت الإيرانية في كف عمل شهادات طبقة المقابس الآمنة لمنصات البريد الالكتروني مثل: *Gmail*، ومواقع التواصل الاجتماعي مثل: *Facebook* و*Twitter* أثناء الحملة الانتخابية عام 2009 وحظرت مواطنيها من استخدام هذه المنصات لبث خطابهم السياسي المعارض).

وتقوم الحكومة الإيرانية بإصدار شهادات طبقة المقابس الآمنة، وكذلك المؤسسات الحكومية، وشركات القطاع الخاص وبإشراف مباشر من قبل جهات حكومية، وهيئات أمنية وأخرى عسكرية بحيث تكون قادرة على التنقير في جميع تفاصيل الأنشطة السيبرانية التي يمارسها المستخدمون الإيرانيون أثناء حضورهم في فضاء الانترنيت.

ولا يتمكن المستخدم العادي من التمييز بين شهادة الترخيص التي تصدرها الجهات ذات الموثوقية في احترام خصوصية المستخدم، وتلك التي أصدرتها جهات غير موثوقة، وتهدف الى اختراق الخصوصية، والتلصّص على الفيض السيبراني، الأمر الذي يوقع المستخدم الإيراني في شباك المراقبة، دون علمه.

وقد أعلنت الحكومة الإيرانية في 23 نوفمبر 2013 عن إصدار خدمة رقمية أطلقت عليها بصمة الثقة السيبرانية *Electronic Trust Mark* والتي تعد الرديف الإيراني لشهادة طبقة المقابس الآمنة *SSL*. وقد تبنت وزارة الصناعة والمناجم ورعت عملية إصدار هذه البصمة السيبرانية، دون غيرها من الجهات الحكومية في المؤسسة الحكومية الإيرانية، رغم عدم وجود صلة مباشرة لأنشطتها مع هذا النشاط السيبراني الذي يرتبط بأمن المعلومات (*ICHR,2014*).

وبصرف النظر عن هوية الجهة التي تصدر هذا النوع من شهادات الثقة السيبرانية، فقد ضمنت الإدارة الحكومية الإيرانية هيمنتها المطلقة على أنشطة جميع الجهات التي تستخدمها، وامتلكت القدرة على التنقير بجميع تفاصيل حسابات المستخدمين، رغم أن الإدارة الحكومية تعد حضور البصمة دليلاً على سلامة الموقع، وروسخ أمنه قبالة أي نوع من عمليات التنصّت، ومراقبة المحتوى، والتزوير الذي قد يمارسه الغير على بيانات المستخدم، باستثناء ممارساتها التي أدرجتها ضمن قائمة الامن الوطني لإيران الذي يقع خارج دائرة الخصوصية والحقوق الشخصية للمستخدم الإيراني.

4 . 1 . 4 . الشبكات الافتراضية الخاصة ـ الايرانية:

الشبكة الافتراضية الخاصة *Virtual Private Network* (*VPN*) تقنية شبكاتية استحدثت لاستثمار القدرات التي توفرها البنية التحتية لشبكات الاتصالات والمعلومات، لإدامة مستوى مقبول من خصوصية البيانات التي يتواصل بها مستخدم الانترنيت مع منصات التطبيقات البرمجية المختلفة.

وقد عمد المستخدمين في البلدان التي تعادي فضاء الانترنيت، وتطبيقاته المنفتحة على الفضاء العولمي، الى استثمار خصائص هذه الشبكات الافتراضية في التسلل عبر الأنفاق السيبراني التي توفرها، وبروتوكولات الأمان الداعمة للفيض الذي يسري في قنواتها، لتجاوز حواجز الحظر السيبراني، والوصول الى منصات التطبيقات التي تلبي حاجاتهم بعيداً عن أنظار منظومات الرقابة والحظر السيبراني الذي تمارسه إدارات الأمن السيبراني في هذه البلدان.

من أجل هذا أدمن المستخدمون الإيرانيون على استخدام الشبكات الافتراضية ـ الخاصة لإدامة الوصول الى مواقع الانترنيت التي تعكف الحكومة الإيرانية على حظر الوصول إليها، أو مراقبة المحتوى السيبراني المودع في مواقعها، أو تقطير عناصرها، من خلال قنوات التشفير التي توظفها البيئة الافتراضية لهذه الشبكات مما يجعلها بمنأى عن أدوات الرقابة وآلياتها السيبرانية (*ICHR,2014*).

ولا زال السجال مستمراً بين الإدارة السيبرانية الإيرانية وبين المستخدمين، فتستمر الإدارة الحكومية ومؤسسات الأمن السيبراني بإيران، في بذل ما في وسعها، للكشف عن الشبكات الافتراضية التي يلجأ المستخدمون الإيرانيون للتسلل من خلالها بعيداً عن أنظار أدوات الحظر والمراقبة، فتسارع الى إغلاق منافذ هذه الشبكات التي تستضاف لدى جهات تقيم خارج حدود الفضاء السيبراني الإيراني، من جهة، وبين استمرار المستخدمين في التنقير عن شبكات افتراضية جديدة، لم تدرج ضمن قوائم حظر الإدارات الأمنية لينالوا من خلال قنواتها الخفية، المزيد من الحضور في فضاء منفتح على المجال العولمي.

ولاستكمال دائرة أمن شبكة الانترنيت الوطنية، باشرت الكوادر السيبرانية الإيرانية بمشاريع لشبكات افتراضية ـ خاصة ذات طابع وطني، تسمح للمستخدم الإيراني في التجول، وفي ظل مراقبة دائمة لمنظومة امنها السيبراني، في فضاء مواقع مختلفة، داخل حدود فضاء الشبكة الوطنية، وخارجها، مع توفر بيئة استعراض، وتجوال رقمي آمن.

أدرجت وزارة الداخلية الإيرانية، الشبكات الافتراضية الخاصة، ضمن الآليات السيبرانية، غير المشروعة، وحظرت استخدامها على المواطنين الايرانيين داخل حدود فضاء الانترنيت في نهايات عام 2012. ولم تمر سوى بضعة أشهر، حتى أعلن المجلس الأعلى لالفضاء السيبراني الإيراني عن إنشاء شبكة افتراضية وطنية، والتي باشرت بطرح خدماتها للمستخدمين الإيرانيين في شهر شباط من عام 2013 على موقع *www.vpn.ir* والذي يوفر خدماته للمواطنين الإيرانيين المقيمين داخل حدود البلاد، ويمنع أي محاولة للوصول الى قنواته السيبرانية من خارج حدود الفضاء السيبراني الإيراني (*ICHR,2014*).

وتستمر الآلة الإعلامية الإيرانية، في الترويج للشبكات الافتراضية الوطنية، لإقناع المستخدمين الإيرانيين بالإقلاع عن الشبكات الافتراضية التي تتوفر بكثرة على مواقع الانترنيت، للتقليل من حجم النفقات التي تسخرها الحكومة لإحكام عملية السيطرة على الفجوات الأمنية ـ المتكاثرة في فضاء الانترنيت، والتي تعمّق التهديدات التي تؤرق الحرس الثوري الإيراني، والمرجعية الإيرانية المحافظة بالوقت ذاته.

ورغم كل ما تفعله الحكومة من خلال آلتها الإعلامية، والجهود التي تبذلها كوادرها التقنية للارتقاء بأداء شبكاتها الافتراضية الوطنية، وتسخير الكثير من المجالات التي تدعم استخدامها، إلا أنها لم تلاقي إقبالاً كبيراً من المستخدم الإيراني، لغياب الثقة بينه وبين إدارته الحكومية على صعيد ملف حرية التعبير عن الرأي، فبقيت مهجورة الا من المستخدمين الذين يمارسون نشاطهم من داخل حدود المؤسسات الحكومية، وبعض منافذ طلبة المرجعيات الدينية.

وفي خطوة لاستثمار شهادات الترخيص الأمنية الوطنية *SSL* توجهت الحكومة نحو مستعرض الويب الوطني سينا *Saina* الذي يعتمد في عمله على ترويج هذه الشهادات في السماح للمستخدمين بعملية استعراض مواقع الويب المختلفة، من خلال قناة الانترنيت الوطنية التي لا تقبل بشهادات أمنية سوى الشهادات التي تصدرها الجهات المعنية بإدارة أمن الفضاء السيبراني الإيراني.

ولا شك أن هذه الشهادات قد ضمنت خلو الموقع مما يخالف الخطاطة العقدية، والسياسية، والأمنية للمؤسسات الثورية الإيرانية، من خلال سلسلة إجراءات الحظر وعمليات تقطير محتوى المواقع. لذا فإن محاولة المستخدم الإيراني بالوصول الى مواقع الويب التي لا تمتلك هذه الشهادة الآمنة سوف يجابه برسائل تحذيرية بعدم إمكانية الوصول بسبب غياب سمة الإبحار الآمن، بينما تغيب هذه الرسالة التحذيرية عندما يسافر المستخدم الى الموقع ذاته من خلال المستعرض الحكومي سينا الذي يحكم قبضته بمراقبة النشاط الذي يمارسه أثناء حضور المستخدم في الموقع ذاته، ويتيح من مادة المحتوى المفردات التي اجتازت قنطرة عملية التقطير.

إن استمرار المستخدمين بالمرور عبر قناة هذا المستعرض الوطني، دون غيره، لضمان وصولهم الى مواقع الويب المختلفة عبر محركات البحث مثل: *Yahoo*، *Google*، *Safari* وغيرها سوف يرسخ الثقة لدى المستخدم الإيراني بشهادة الترخيص الآمن ذات الصبغة المحلية، أو القبول بها، كأمر مفروغ منه، مما سيسهم في نجاحها، والترويج لاستخدام المستعرض الإيراني بدلاً من غيره. وبذلك ستنتظم مسارات الفيض السيبراني للمستخدمين الإيرانيين في سفرها عبر قنوات النفق الحكومي الذي تهيمن على نبضاته السيبرانية مجسّات الرقابة الحكومية، بمختلف اختصاصاتها.

وتظهر الوثائق الحكومية أن عملية إصدار هذه الشهادات قد بدأت بالتكاثر من 25,000 شهادة في عام 2011 لتزيد على 500,000 شهادة خلال عام 2014، الأمر الذي يؤكد رغبة الحكومة في إنجاح مشروعها وتوسيع رقعة استخدام هذه الشهادات، في سعيها لتمهيد مستلزمات إنجاح شبكة الانترنيت الوطنية. بيد أن هذا النمو لا زال متواضعاً في عديده قبالة عشرات الملايين من الشهادات غير الحكومية التي يميل الى استخدامها المواطنين الإيرانيين عند ابحارهم في فضاء الانترنيت.

4 . 2 . التطبيقات والمنصّات الإيرانية البديلة:

بذلت الإدارة السيبرانية في إيران، وبمختلف مؤسساتها القاطنة في وزارة تقنية المعلومات والاتصالات، ومراكز بحوث المعلومات والصناعة البرمجية، على التوازي مع توفير دعم مستمر لشركات القطاع الخاص جهوداً استثنائية لاصطناع وتوفير مقومات بيئة برمجية ثرية بمنصات التطبيقات الداعمة لمستخدمي الانترنيت سواء بواسطة الحواسب أو الهواتف المحمولة لضمان تحقيق انجذاب نحو البيئة الوطنية وصرفهم عن إغراءات التطبيقات التي تطرحها الشركات العالمية التي تهيمن على بيئة الاتصال والتواصل في فضاء الانترنيت.

وقد حاولت الجهات المطورة محاكاة وتقليد التطبيقات ذائعة الصيت على المستوى العولمي، وإصدار تطبيقات محلية تقاربها، الى حد مقبول، على صعيد الخدمات المطروحة، وبتصاميم واجهات توحي للمستخدم بعدم غربته عما يستخدمه الغير من مستخدمي الانترنيت في دول المنطقة.

ورغم أن هذه المحاولات لا زالت في بداياتها، إلا أنها بدأت يوماً بعد يوم بتوفير كم كبير من التطبيقات المحلية، التي تناظر تلك التي يحفل بها الفضاء العولمي للانترنيت، ويتوقع أن توفر بيئة داعمة لإنجاح الانترنيت الوطنية التي تروم إيران بنشر سلطان فضائها البديل عن فضاء الانترنيت الوافدة من دول معادية، وتحفل مواقعا بخطاب يناهض خطاب الثورة الإسلامية وثقافاتها.

لقد وظفت هذه البرمجيات لإزاحة المستخدمين الإيرانيين من فسحة فضاء الانترنيت العولمي من خلال توليد قناعات لديهم بنجعتها وقدرتها المميزة على التخاطب باللغة الفارسية، وتوافقها الكبير مع حس المواطن الإيراني. وتأمل في ان يسهم نجاح هذه التطبيقات في تقليل حجم الضغوط المالية والتقنية التي تتطلبها عملية حجب المواقع، والرقابة الذكية، التي باتت تثقل كاهل الحكومة مع زيادة حجم الكلف المطلوبة لتحقيق هذه الغاية (تضاعفت التخصيصات المالية لأمن المعلومات بمقدار 12 ضعفاً في ميزانية عام 2014) (*SMO,2014,a*)، وتكاثر التطبيقات التي توفر للمستخدم فرصة اختراق وتخطي جدران الرقابة التي لم تعد مجدية سوى لفسحة زمنية قصيرة، ثم تتراجع قدراتها قبالة التطور التقني المستمر في مجال تقنيات الاختراق وتجاوز جدران الكف والحظر.

4 . 2 . 1 . نظام التشغيل الإيراني زمين:

يعد نظام التشغيل *Operating System* البوابة الرئيسة التي يطل منها المستخدم على الفضاء المحوسب، والتربة التي تستنبت فيها مختلف أشكال التطبيقات الحاسوبية التي يوظفها المستخدم لإدارة نشاطه ضمن منصة الحاسوب الذي يطل من خلاله على فضاء الانترنيت بالوقت ذاته.

لقد ادركت الحكومة الإيرانية أهمية نظم التشغيل في الهيمنة على توجهات المستخدمين الإيرانيين نحو التطبيقات البرمجية التي تهيمن على انتاجها عدوتها اللدود (الولايات المتحدة) لذا فقد عقدت العزم على استنهاض قدرات كوادرها السيبرانية، لإنتاج نظام تشغيل وطني، لا يتوافق إلا مع تطبيقات إيرانية صرفة، تبعد المستخدم الإيراني، شيئاً فشيئاً، عن التطبيقات التي تنتجها كبريات الشركات المنتجة للتطبيقات البرمجية، كما أن استخدامها سيسهم في انتزاع المستخدم الإيراني من الفضاء المحوسب العولمي باتجاه فضاء إيراني صرف، لا يستنبت الا البذور التي رعتها الحكومة الإيرانية في مناخ ثقافة الثورة الإسلامية، وبإشراف المنظومة العقدية الحوزوية، والمنظومة الأمنية للحرس الثوري الإيراني.

منذ بدايات العقد الأول من الألفية الجديدة، باشرت مؤسسة تقنية المعلومات *ITO* بالتعاون مع مركز إيران لبحوث الاتصالات *ITRC* بالعمل على تصميم وتنفيذ نظام تشغيل وطني، يرتكز الى منصة الموارد المفتوحة، التي تعتمد نظام التشغيل *Linux*، أطلق عليه زمين *Zamin*.

وقد تجلى اهتمام الإدارة الحكومية بنظام التشغيل الجديد من خلال توطين فريق العمل الذي عكف على تصميمه ضمن مكتب التعاون التقني بالقصر الرئاسي أثناء ولاية الرئيس السابق محمود أحمد نجاد. واستكملت وثائق نظام التشغيل الجديد عند نهاية عام 2010، وعرضت على الهيئة الوطنية الاستشارية لإقرارها، وبعد أن تجاوزت هذه المرحلة تجاوز نظام التشغيل الاختبار وأقر استخدامه على المستوى التجاري بديلاً لنظام التشغيل الشهير *Windows*.

ولد الإصدار الأول لنظام التشغيل زمين في نوفمبر 2012، وخصص للاستخدام على الحواسب المنضدية، ومع بدايات عام 2013 ولد الإصدار المتوافق مع الأجهزة المحمولة. وقد هرعت الحكومة الإيرانية الى حظر استخدام نظام التشغيل *Windows* في حواسب مؤسساتها المختلفة، وخلال مدة لا تتجاوز ستة أشهر.

بيد أن هذا الاجراء قد عكس بجلاء تسرع الإدارة الحكومية في التوقيت الزمني لتنفيذ عملية الحظر، لأن عملية التحوّل ليست سهلة كما يتوهمها البعض، بسبب تغلغل تطبيقات التي تعمل تحت مظلة منصة نظام *Windows*، كما أن نظاماً تشغيلياً لا يتجاوز عمقه المعرفي بضعة سنوات، وأنجز بواسطة كوادر محلية، لا يمكن أن ينافس نظاماً تشغيلياً تجاوز عمره بضعة عقود، وقد تناسل استخدامه على عموم رقعة الاستخدام العولمي المحوسب، وتجاوز قنطرة جميع تطبيقات دول العالم المتحضر.

لذا نتوقع أن يتأخر تنفيذ عملية الحظر على أرض الواقع الإيراني، كما أن ضمان قبول المواطن الإيراني بالتحول نحو نظام سيحكم قبضته على جميع الأنشطة التي يمارسها، داخل حدود الفضاء السيبراني وخارجه، يعد أمراً شبه مستحيل.

4 . 2 . 2 . مستعرضات ومحركات بحث وتطبيقات إيرانية:

بصورة عامة، ظهرت مجموعة متنوعة من البرمجيات المناظرة لمحركات البحث وتطبيقات الإبحار السيبراني في خطوة مناظرة لم اتبعته الصين لجذب مواطنيها الى تطبيقات تناظر محركات البحث التي طرحتها الشركات البرمجية العملاقة مثل *Google*، *Yahoo*، أو حزم برمجية تطبيقية مثل *Microsoft Office*، وغيرها من البرمجيات التي لم يعد المستخدم

المعاصر قادراً على الاستغناء عن خدماتها الداعمة لأنشطته المختلفة التي يمارسها داخل نطاق عمله، أو في إدارة تفاصيل أنشطته اليومية.

كما تزايد الاهتمام بالمنصات والتطبيقات البرمجية التي تناسلت في بيئات الهواتف الذكية (بيئتي *IOS* و*Android*) وسحرت المستخدمين وانتزعتهم من بيئة الحاسب *Windows* باتجاهها.

بدأت بعض هذه التطبيقات المحلية بجهود ذاتية ـ محلية منذ بداية العقد الأول من الألفية الجديدة، بيد أن وزارة تقنية المعلومات والاتصالات الإيرانية قد باشرت منذ عام 2014 بتبني سياسة لدعمها من خلال توفير مختلف أشكال الأسناد لمراكز البحوث وصناعة التطبيقات البرمجية الحكومية، والشركات البرمجية الخاصة لتشجيع التوجه نحو بناء منصات برمجية وتطبيقات وطنية تحاكي التطبيقات التي باتت تجذب المستخدمين، فتنتزعهم من بيئتهم باتجاه بيئة تخالف القيم التي تنادي بها الثورة الإسلامية (*SMO,2014,a*).

وبدأت هذه المنصات تجذب الكثير من المستخدمين داخل حدود الفضاء السيبراني في إيران، بيد أنها لم تنجح في انتزاع المستخدم الإيراني، أو تقنعه بمقاطعة المنصات والتطبيقات البرمجية التي تستوطن بيئة الانترنيت العولمية. وقد توزعت التطبيقات البديلة بين منصات شبكات التواصل الاجتماعي، ومحركات البحث، وبرامج التواصل الهاتفي، وغيرها من التطبيقات التي يحفل بها الفضاء السيبراني المعاصر ـ أنظر الجدول (2 - 20).

الجدول (2 - 20) ـ المنصات والتطبيقات البرمجية الإيرانية البديلة.

الفئة	التطبيق العولمي	التطبيق الإيراني البديل	التفاصيل
محركات بحث وتصفح	Google	Parsijoo	محرك بحث إيراني ظهر عام 2010 بوصفه بديلاً للموقع العملاق *Google*.
	Firefox	Saina	برنامج تصفح بديل لبرنامج *Firefox* في بداية عام 2011.
	Google Analytics	Webgozar	برنامج داعم لمحرك البحث *Google* ظهرت إصدارته الأولى عام 2003.
منصات شبكات التواصل الاجتماعي والدردشة الالكترونية	Facebook	Facenama	أصدر هذا البرنامج بوصفه بديلاً منافساً لمنصة *Facebook* للتواصل الاجتماعي عام 2011 وتجاوز عديد مستخدميه عام 2013 المليون مستخدم.
		Cloob	أبصر النور هذا التطبيق عام 2004 بوصفه بديلاً لموقع التواصل المحلي *Orkut* والذي حجب في العام ذاته. ويتمتع بميزات وخدمات تحاكي تلك التي نجدها في منصة *Facebook*.
	You Tube	Parat	منصة تبادل فيديوي بسمة تناظرية تحاول توفير خدمات مقاربة لخدمات موقع You Tube باشرت عملها في عام 2011 لتجاوز عقبة الصعوبة المصاحبة لحظر محتوى المنصة الأصلية.
	Instagram	Lenzor	منصة تواصل صوري أصدرت عام 2014 بوصفها بديلاً لمنصة Instagram حيث يمارس عملية تقطير المحتوى من المشاهد غير اللائقة.

الفئة	التطبيق العولمي	التطبيق الإيراني البديل	التفاصيل
	Dialog	We Chat	برنامج للدردشة الالكترونية بديل للبرنامج الصيني ظهرت إصدارته الأولى عام 2014.
منصات تطبيقات برمجية	iTunes	Beep Tunes	في بداية عام 2014 أصدرت وزارة الثقافة والإرشاد الديني ترخيصها لتطبيق Beep Tunes وهو البرنامج الإيراني البديل لتطبيق iTunes الذي يستخدم في الهواتف المحمولة، والحواسب اللوحية وحواسب شركة *Apple* الأمريكية الشهيرة.
	Google Play	Café Bazar	متجر بديل لمتجر تطبيقات شركة Google الذي خصصته لترويج تطبيقات نظام Android أصدر في عام 2011.
	App Store	Sibche	متجر لتطبيقات نظام Android ظهرت إصدارته الأولى عام 2011.

المصدر: *SMO,2014,c*.

حققت بعض هذه التطبيقات نجاحاً ملموساً على صعيد اجتذاب شريحة واسعة من المستخدمين الإيرانيين، بعد أن اصطنعت لهم بيئة برمجية حاضنة تحاكي المنصات والبيئات البرمجية الغربية. ومن هذه التطبيقات تطبيقات التواصل الاجتماعي *Facenama & Cloob* بينما أخفقت أخرى في تحقيق الغاية المرجوة من إصدارها مثل منصة *Parat* التي أطلقت بديلة لموقع *You Tube* حيث لم تنجح بجذب المستخدمين من إيران. إلا أن هذه التطبيقات مجتمعة لم تنجح في فطام المستخدم الإيراني، أو صرفه عن المواقع التي حاولت محاكاتها، بحيث بقيت الكثير من القيادات السياسية والمرجعيات تستخدم التطبيقات التي أنتجت في الغرب.

بالمقابل أقبلت الكثير من الشخصيات الإيرانية مثل: هاشمي رفسنجاني، ووزير تقنية المعلومات والاتصالات محمد فايزي، وآية الله بهجت فوماني على استخدام منصات التواصل الاجتماعي المحلية كونها تعد بيئة تواصلية ملتزمة بقيم الثورة الإسلامية، وللإعلان عن مشروعية استخدام بنظر الحكومة والمرجعيات الحوزوية بالبلاد.

وفي بداية شهر فبراير من عام 2015 أعلن بارات جانباري (وكيل وزير تقنية المعلومات والاتصالات لشؤون التخطيط والتحكم الاستراتيجي) أن إيران ستقوم بتشغيل محرك بحث جديد *Search Engines* بمناسبة الاحتفال بذكرى تأسيس الدولة الإسلامية (1-11 فبراير 2015). وقد أطلق على المنصة البرمجية الجديدة *Gorgor*. خصصت ميزانية بلغت 60 مليون دولار لدعم فريق التطوير من جامعة الامام الحسين، مع توفير دعم إضافي لمحرك البحث الشهير *Parsijoo* في إصدارته الجديدة التي عكف عليها فريق من جامعة يزد وبالتعاون مع الوزارة ذاتها، التي دعمت المشروع بأكثر من 150 خادم الكتروني (*SMO,2015,a*).

وبعد مدة قصيرة أعلن عن محرك بحث صممته وباشرت بتشغيله وزارة تقنية المعلومات والاتصالات، وأطلق عليه *Yooz*. ويستطيع محرك البحث الجديد التنقير في أكثر من مليار صفحة ويب قامت مضيفات الوزارة بأرشفتها وإعداد فهارسها الداعمة لعمليات البحث، خلال بيئة وطنية آمنة، تخلو من أي عملية حظر على المحتوى السيبراني لهذه المضيفات (*SMO,2015,b*). على صعيد متصل، أعلن مهدي شجري (مدير قسم تقنية المعلومات في كلية الحاسب وهندسة تقنية المعلومات في جامعة أمير كبير للتقنية) أن عام 2014 سيكون نقطة البداية لمشروع إنتاج برنامج وطني تتعاون على إكماله مجموعة من الجامعات الإيرانية. وسيتضمن هذا المشروع تصميم وإنتاج مستعرض وطني *National Browser* عبر 18 مرحلة، انتهت الأولى منها في النصف الأول من عام 2014، وشرع فريق العمل بالمرحلة

الثانية. وسيحتوي المستعرض على أداة لكف عمليات التصيّد السيبراني *Phishing* لضمان حماية المستخدم السيبراني من هذا الاختراق. وسيطلق على المستعرض الجديد اسم ناب *Naap* (*SMO,2014,c*).

ولإنجاح عملية محاكاة المنصات والتطبيقات البرمجية بواسطة الكوادر التقنية والأكاديمية الإيرانية فقد خصصت الحكومة 32 مليون دولار لسنة 2015، مع مبلغ إضافي لعام 2016 سيصل الى 42 مليون دولار. وتشارك أكثر من 20 شركة إيرانية في عمليات تطوير محركات البحث الوطنية، والتي ستقيم في شبكة الإنترنيت *SHOMA* (*SMO,2015,a*).

وبدا أن الحكومة قد قاربت بلوغ أهدافها، بعد أن باشرت الكثير من المنصات البرمجية البديلة في قطاع شبكات التواصل الاجتماعي، والتجارة الالكترونية، بالعمل ونجحت باجتذاب الكثير من المستخدمين الإيرانيين الذين أثقلتهم إجراءات الحظر وتقطير المحتوى، على التوازي مع تصاعد أنشطة الملاحقة للناشطين، وتصعيد الأحكام الجنائية بحق المخالفين.

وقد بدا واضحاً أن الحكومة تريد التخفيف من وطأة التخصيصات المالية الهائلة لإدامة عملية حظر المواقع، وتقطير المحتوى، التي لم تنجح أمام طرح تقنيات بديلة لتجاوز عمليات الحظر، لتعاود معالجاتها الأولية في تقليل سرعة خدمة الانترنيت الى مستويات تحول دون وصول المستخدم الإيراني الى المواقع المحظورة دون الحاجة الى نظم متطورة للحجب السيبراني. كذلك فإن تحويل مضيفات الخدمة الى داخل حدود البلاد سيوفر المزيد من العملة الصعبة، وسيدعم نشوء سوق نشط لمراكز البيانات في إيران.

لقد اتضحت متغيرات المعادلة الحاكمة لتوفير الخدمة أو حجب بعض مواقعها، أو ايقافها بالكلية كما حصل أثناء الحملة الانتخابية لعام 2009 وعام 2013. ان الاستمرار بهذا النهج سيحمّل الحكومة المزيد من الانفاقات مع تصاعد القلق من وجود أكثر من فرصة لحصول فجوة رقمية تفشل الإجراءات الأمنية الاحترازية فتذهب الأموال المخصصة سدى، أما التحول الى البيئة الأمنة لشبكة الانترنيت الوطنية *SHOMA* فسيعفي الحكومة والمؤسسة الأمنية لالفضاء السيبراني من القلق المستمر، كما أنه لن تكون هناك حاجة لعمليات الحظر أو التقطير على محتوى قد عولجت مادته بعناية على موارد رقمية تقيم داخل حدود سلطة الثورة الإسلامية، كما ان هذه الموارد قد قطعت ارتباطاتها بالكلية عن النسيج الشبكاتي العولمي للانترنيت.

ونود التأكيد على أن الكوادر الإيرانية رغم نجاحا في إصدار تطبيقات متعددة تحاكي المنصات والتطبيقات البرمجية الغربية، إلا أنها لا تمتلك خبرة معلوماتية عميقة كالتي تمتلكها كوادر الصين وشركاتها العريقة مثل *Huawei & ZTE*الأمر الذي صبغ هذه التطبيقات بالقصور في كثير من تفاصيل أدائها. نذكر على سبيل المثال لا الحصر أن هيئة تقدير المحتوى السيبراني الجنائي *CDICC* الإيرانية التي تنهض بمهمة تحديد المحتوى الاجرامي ـ السيبراني قد أعلنت عن حظر التطبيق *WeChat* في شهر كانون الأول من عام 2013 بحجة تسريب التطبيق لمعلومات شخصية عن المستخدم نتيجة للإعلان عن قائمة المستخدمين القريبين، والذي يشكل سلوكاً يتعارض مع اخلاقيات وقيم الثورة الإسلامية. بيد أن إطلاق النسخة الإيرانية *Dialog* وبمباركة من المؤسسة الحكومية والدينية كونه بديل آمن للتطبيق الأصلي قد أصيب بانتكاسة لأن التطبيق الإيراني الذي اكدت الهيئات الرقابية بتوافقه مع القيم السامية تبين أنه يوفر الخاصية ذاتها التي سببت لغطاً كبيراً ونجم عنها حجب الموقع الأصلي والتوجه نحو إصدار تطبيق برمجي محلي بديل! (*SMO,2014,c*).

5 . شبكة الانترنيت الإيرانية على أرض الواقع:

لقد ترسخت القناعة لدى جميع مؤسسات الحكومة الإسلامية بإيران، وعلى رأسها المجلس الأعلى للثورة الإسلامية، والحرس الثوري الإيراني، والمرجعيات الدينية التي ترعى حمى العقيدة الشيعية وخطاطتها المفاهيمية، أن هناك تهديداً قائماً لمكتسبات الثورة وبنيتها العقدية، وما تحقق من تقدم تقني على صعيد الملف النووي وملف الآلة العسكرية الوطنية، تمارسها الدول المعادية للثورة، وعلى رأسهم الولايات المتحدة الأمريكية والكيان الصهيوني، ودول غربية أخرى تناصبها العداء وتحرص على زعزعة النظام. وأن هذا التهديد قد بدأ يتسلل من القنوات المفتوحة لفضاء الانترنيت الذي تغلغل في معظم مفاصل الدولة الإيرانية، بالإضافة الى تزايد إقبال المواطنين الإيرانيين على الحضور في هذا الفضاء الذي جعل من الفضاء الوطني الإيراني مجالاً خصباً لتسلل الجهات المعادية عبر مستويات متعددة من قنوات الاتصال والتواصل السيبراني.

لذا لم يتوفر خيار آخر امام الإدارة الحكومية الإيرانية، سوى التوجه نحو إنشاء بنية تحتية وطنية لدعم جميع أشكال عمليات التواصل والاتصال السيبراني بالبلاد، والتوجه نحو توفير كفاية شبكاتية داعمة لجميع أشكال الأنشطة السيبرانية بالبلاد، بعيداً عن فضاء الانترنيت المشحون بالتهديدات السيبرانية التي يمكن أن تتسلل من العقد السيبرانية التي تربط النسيج الشبكاتي الإيراني، بالنسيج العولمي لشبكة الانترنيت.

من اجل هذا سعت الحكومة الى إنتاج نسخة إيرانية من فضاء الانترنيت في سعيها لتحقيق قنوات آمنة لتداول المعلومات التي تخص أمن الدولة (على المستويين العسكري والتقني)، من جهة، وحجب المواقع والمحتوى الذي يتنافى من مبادئ الثورة الثقافية التي جاءت بها الثورة الإسلامية في إيران، وحماية المواطن الإيراني من آثارها الضارة (بحسب الخطاطة العقدية والسياسية التي تبنتها الحكومة الإيرانية منذ عقود).

في البداية حاولت التقليل من آثار التهديدات المحتملة من خلال تبني سياسة أمنية وطنية أجبرت أكثر من 90% من مواقع مؤسسات الدولة ومصارفها على التحوّل الى مضيفات خدمة داخل حدود إيران، لضمان السيطرة على المرور السيبراني الوطني ضمن حدود سيطرة الدولة. ثم توجهت نحو اعتماد مبدأ تقليل سرعة خدمة الانترنيت لكفّ المستخدم الإيراني عن الوصول الى المواقع التي تعدها الحكومة منافية لخطاطة ثقافة الثورة الإسلامية، ثم التوجه نحو توظيف تقنيات رقمية متقدمة لحجب المواقع، وتقطير المحتوى السيبراني، بوصفها خطوات تمهيدية للتقليل من الآثار المحتملة للتهديدات السيبرانية المادية والمعنوية لحين اكتمال مشروع شبكة المعلومات الوطنية، والتي أطلق عليها في أحيان أخرى شبكة الانترنيت الوطنية، أو شبكة الإنترنيت الحلال، والتي انصبغت أخيراً باسم شبكة المعلومات الوطنية *SHOMA*.

5 . 1 . الخطاطة السيبرانية لشبكة المعلومات الوطنية SHOMA:

في البداية، كان المبدأ الذي استند إليه قرار إنشاء شبكة معلومات وطنية، هو إقامة فضاء اتصالي يتيح للمواطن الإيراني أن يتواصل ويتصل من خلالها بالآخر، ضمن مناخ رقمي آمن، بحسب المبادئ العامة لثقافة الثورة الإسلامية. بيد أن تغلغل خدمة الانترنيت، وتطبيقاتها الجذابة الى أعماق نفوس المستخدمين، والتصاقهم بفضائه المفتوح، وفي ظل الجو المحافظ الذي حرصت الثورة الإسلامية على ترسيخ جذوره في الحياة اليومية للمواطن الإيراني، قد أسهم في تزايد حجم الفجوة بين فضاء الانترنيت العولمي، والفضاء الذي طالبت بها جهات متعددة تهيمن على صناعة الكثير من القرارات المهمة التي تخص الدولة والمجتمع الإيرانيين.

لقد أطلقت مؤسسة الحرس الثوري الإيراني، والمرجعيات الدينية الكثير من المطالب التي لا تزيد عن كونها تصورات غير موضوعية في دائرة تقنية المعلومات والاتصالات بسبب مستوى التقنيات المطلوبة لتحقيق هذه الغايات، قبالة

بيئة اقتصادية تعاني من آثار حصار خارجي، مع شحة التخصيصات بسبب العقوبات المتعددة التي فرضت على إيران. ومما عمّق حجم هذه التحديات بروز سمة التداخل والتجاذب بين المجلس الأعلى للثورة الإسلامية في إيران، والإدارة الحكومية المتأرجحة بين النهج المحافظ لأحمدي نجاد، والنهج المنفتح لحسن روحاني، مع الضغوطات التي تمارسها مؤسسة الحرس الثوري الإيراني، من جهة، والضغوط ذات الصبغة العقدية التي تمارسها الحوزات العلمية والمرجعيات العلمية في إيران، بتشويه معالم فضاء القرار الإيراني حول تحديد ماهية وحدود الخطاطة السيبرانية الحاكمة لهوية وخصائص، واهداف شبكة المعلومات الوطنية *SHOMA*.

إن وجود أكثر من مؤسسة تدير دفة سياسة وأمن الحكومة الإسلامية في إيران، مع وجود مستويات متعددة من الصلاحيات المنفردة التي تمارسها بعض هذه المؤسسات بمعزل عن بقية المؤسسات، قد كلّف الإدارة الحكومية المزيد من التخصيصات المالية التي خصصتها بعض هذه المؤسسات لمشاريع شبكاتية، قد تعد إضافات مشوهة لنظام شبكة *SHOMA*، أو قد تؤثر بصورة معكوسة على الخطاطة التقنية للشبكة الوطنية للمعلومات.

فعلى سبيل المثال، تمتلك مؤسسة الباسيج الإيرانية *Basij* شبكة معلومات منفصلة في عملها عن العقد السيبرانية لشبكة المعلومات الإيرانية *SHOMA*، وتقوم بمهمة نقل البيانات، وتوفير فضاء اتصالي بين منتسبي هذه المؤسسة الأمنية بمعزل عن الفضاء الاتصالي الذي ستوفره الإدارة الحكومية للمواطن الإيراني، وبقية مؤسساتها الحكومية (*SMO,2014,d*). من جهة أخرى، فقد صرّح عبد الرضا رحماني فاضل (وزير الداخلية الإيراني)، في بداية عام 2014، أن شبكة الإذاعة والتلفاز الإيرانية *IRIB* ستقوم بإطلاق نظاماً جديداً للشبكات الافتراضية *Virtual Networks* والتي ستغطي اكثر من 10 آلاف هيئة محلية في عموم المحافظات الإيرانية، والتي ستسمح للمواطنين في هذه الأماكن المتباعدة للتواصل فيما بينهم وتبادل المعلومات عبر نسيج هذه الشبكة السيبرانية. ولم يتضح من تصريح الوزير المذكور الصلة التي تربط مثل هذا المشروع مع شبكة المعلومات الوطنية *SHOMA*، وهل أن هذه الشبكة ستعمل بمعزل عن نسيج الشبكة الوطنية للمعلومات (*SMO,2014,a*). وعلى صعيد آخر، أعلن وكيل وزير تقنية المعلومات والاتصالات الإيراني (برات غانباري) في منتصف عام 2015 عن إطلاق شبكة المعلومات *Tavna* وهي عبارة عن الشبكة المحلية الرئيسة التي سترتبط بين العاصمة طهران ومدينة أصفهان، وباستخدام أدوات اتصالات ومعلومات مصنعة في إيران. ولم تفصح الوزارة عن طبيعة العلاقة بين هذا المشروع، ومشروع شبكة الانترنيت الوطنية *SHOMA* (*SMO,2015,c*).

وبالوقت ذاته، لا زال الغموض يلف بماهية مكونات شبكة الانترنيت الوطنية الإيرانية *SHOMA* وطبيعة الخدمات التي ستوفرها للمستخدم الإيراني بحيث تجذبه من فضاء الانترنيت العولمية. ولم يتضح كيفية طرح المحتوى الملتزم بثوابت وقيم الشريعة الإسلامية، وبمبادئ ثقافة الثورة الإسلامية، رغم كثرة التصريحات التي أطلقها مسؤولين في حكومة الرئيس السابق (محمود أحمدي نجاد)، والرئيس الحالي (حسن روحاني). فالجميع يطرح تصريحات غامضة، وتتسم بأوصاف فضفاضة، ووعود بتوفير بيئة آمنة على المستويين الأخلاقي والسياسي، لم يبرز للعيان ما يؤكدها لغاية هذا التاريخ.

ولعل من الشواهد التي تؤكد ما ذهبنا إليه، تباين التصريحات التي يطلقها المسؤولين، بين الحين والآخر، حول الشبكة وهويتها. فبحسب تصريحات محمد انتظاري (سكرتير المجلس الأعلى لالفضاء السيبراني) أن دخول شبكة الانترنيت الوطنية *SHOMA* بالخدمة، لن يقطع عقد ارتباط المستخدمين الإيرانيين بشبكة الانترنيت العولمية، وأن الشبكتين ستعملان على التوازي في توفير الفضاء الاتصالي للمستخدم الإيراني، الأمر الذي يناقض ما تهدف إليه الحكومة في عزل فضائها السيبراني عن الفضاء العولمي للانترنيت (*SMO,2014,d*).

كذلك خرج الكثير من المسؤولين بتصريحات لوسائل الاعلام تؤكد غياب الاتفاق بصدد خطاطة شبكة *SHOMA*، منها الخلاف المستديم بين المجلس الأعلى لالفضاء السيبراني وإدارة وزارة تقنية المعلومات والاتصالات بصدد النتائج المتوقعة من تشغيل الشبكة، وجملة من خصائصها التقنية (*SMO,2014,c*).

ويكاد يصح الأمر ذاته بصدد تصريحات المسؤولين حول نسبة إنجاز كل مرحلة من مراحل تنفيذ المشروع، وتوقيت مباشرة الشبكة بتوفير خدماتها للقطاع الحكومي والخاص[57]، ولعموم المواطنين الإيرانيين[58]، وتحديد هوية المحافظات المشمولة بخدماتها السيبرانية؟، وهل ستعمل مع وجود خدمة الانترنيت التقليدية؟، أم أن شروعها بالعمل سيؤدي الى انفصال إيران عن الفضاء العولمي للانترنيت؟، وهل ستتوفر أدوات كافية في فضاء شبكة *SHOMA* تلبي حاجات المستخدم الإيراني في الفضاء الجديد[59].

وخلاصة القول في هذا المقام، فإننا نتوقع أن تستمر سياسة إدارة فضاء الانترنيت في تأرجحها بين أطراف متناقضة، بسبب التنازع المستمر بين عدة أطراف متناحرة، تتبوأ ساحته جهات متعددة، بعضها مستوطن في مؤسسة الحرس الثوري الإيراني، وأخرى في المؤسسة الحكومية، وثالثة تهيمن على المؤسسات والمرجعيات الدينية، والذين ينصاعون جميعاً لسلطة المرشد الأعلى للثورة الإسلامية آية الله علي خامنئي.

ورغم تباين عناصر هذه المعادلة المتناقضة، والصعبة، في الوقت ذاته، ما انفك الإيرانيون بجميع فئاتهم، وانتماءاتهم، ملتصقين بهذه الخدمة التي حققت لهم بعض أحلامهم، في الاطلاع على عوالم منعت من الحضور امام اعينهم، ولم تعد نبضاتها تصل الى أسماعهم. وقد استشرت حمى الانترنيت في أبدانهم، وتوغلت في نفوسهم، بحيث لم تعد أدوات الحظر، وتقطير المحتوى قادرة على حجزهم عن تخوم الخدمة، فاستخدموا جميع أدوات التسلل السيبراني، وبدأوا ينقرون بأظافرهم قنوات رقمية لتكون موارداً لتسلل النبضات من المواقع المحظورة الى أدواتهم الاتصالية.

ويمكن أن نتلمس هذا التناقض، حتى في السياسة التي ينتهجها الرئيس حسن روحاني. فبالرغم من زيادة حجم الميزانية الحكومية التي خصصت لقطاع المعلومات والاتصالات الى مستويات غير مسبوقة منذ عدة سنوات، فإن هذه الأموال قد تنازعتها الأطراف المتناحرة، فوظف الإصلاحيون شطرها للارتقاء بمستويات البنية التحتية الاتصالية، وزيادة سعة حزمة خدمة الانترنيت، وإدخال خدمة 3G للهواتف المحمولة، بينما استخدم أنصار الثقافة الثورية، والموالين للمرجعيات المحافظة والمتشددة الشطر الآخر لتطوير نظم الحجب والمراقبة، وتكثيف عمليات تقطير المحتوى، والسعي الى الحد من توسيع دائرة خدمة 3G بسبب اعتقادهم أن توفير خدمة الانترنيت السريع بالهواتف المحمولة يعد نهجاً مخالفاً لمبادئ الشريعة الإسلامية وثوابتها.

---

[57]. على صعيد ارتباط المؤسسات الحكومية بشبكة الانترنيت الوطنية، ذكر علي أصغر أنصاري (وكيل مؤسسة تقنية المعلومات في إيران) أن أكثر من 130 مؤسسة حكومية سوف تتقاسم المعلومات من خلال ارتباط عقدها السيبرانية مع شبكة *SHOMA* عند نهاية الخطة الخمسية الوطنية للسنوات (2012–2016). وأضاف أن السنة الثانية من الخطة ذاتها سوف تشهد ارتباط حوالي 150 ألف مؤسسة حكومية بنسيج شبكة الانترنيت الإيرانية (*SMO,2015,c*).

[58] . أشار نصر الله جاهنجارد (وكيل وزير تقنية المعلومات والاتصالات) أن شبكة الانترنيت الوطنية *SHOMA* جاهزة للعمل، وأنها ستكون قادرة على تجهيز خدمة الانترنيت لجميع المواطنين بالمحافظات الإيرانية. وتخطط الوزارة لتجهيز 60 % من المساكن بالخدمة الجديدة، على التوازي مع تجهيز 100 % من المؤسسات الحكومية (*SMO,2015,b*).

[59] . وفق ما جاء في تصريح وزير تقنية المعلومات والاتصالات، في الربع الأول من عام 2014، فقد عكفت ثلاث جامعات إيرانية مجموعة من مراكز البحث الوطنية بالتعاون مع وزارته في العمل على مشروع لنظام التقطير الذكي *Intelligent filtering System* والذي سيوفر للإدارة الحكومية الإيرانية فرصة حجب وتقطير محتوى مجموعة من مواقع الويب التي تطرح مواداً إباحية تخالف الشريعة الإسلامية، وأن المشروع الريادي للشبكة الإيرانية سوف يباشر بربط خمس أو ست مدن بفضاء *SHOMA* السيبراني في 22 سبتمبر 2014 (*SMO,2014,b*).

5 . 2 . مراحل تنفيذ مشروع شبكة الانترنيت الوطنية *SHOMA*:

مرت شبكة الانترنيت الوطنية بعدة مراحل نتيجة لعدم وضوح خطاطتها لدى الجهات التشريعية بالبلاد، وتجاذب أطراف عدة في تحديد هويتها، وخصائص فضاءها السيبراني. وروجعت مضامينها التقنية، وطبيعة الخدمات التي ستوفرها، ومادة المحتوى التي ستستضيفه في فضائها السيبراني خلال السنوات 2009-2014 وخلال الفترة الانتقالية بين ولاية محمود احمدي نجاد، ثم الدكتور حسن روحاني.

وقد خطط لتنفيذ المرحلة الأولى من شبكة الانترنيت الوطنية عام 2012، وذلك من خلال العمل على فصل شبكات المعلومات المحلية في إيران، وضمان عملها بمعزل عن شبكة الانترنيت العولمية. وشملت هذه المرحلة تجهيز 10 ملايين مستخدم إيراني بخدمات معلوماتية تصل سرعة حزمتها الى 20 *Mbps*، كما ان لوزارة تقنية المعلومات والاتصالات الإيرانية خطط مستقبلية ستؤمن إيصال الخدمة الى جميع مستخدمي الانترنيت الوطنية خلال المستقبل القريب.

أما المرحلة الثانية فقد خطط للانتهاء منها في نهاية شهر مارس من عام 2014، على أن تشهد استضافة جميع مواقع الويب الإيرانية لدى المضيفات المحلية، التي تستوطن الرقعة الجغرافية للبلاد.

وتأتي المرحلة الثالثة، والتي يؤمل انتهاؤها قبل نهاية عام 2016، إيذاناً باستكمال جميع منصات التطبيقات البرمجية الوطنية التي تدعم جميع اشكال الخدمات السيبرانية التي يروم المواطن الإيراني الحصول عليها عند دخوله الى فضاء الانترنيت الإيراني، مع إحكام الإدارة السيبرانية الوطنية سيطرتها وإدارتها لجميع الأنشطة السيبرانية التي تسافر في قنوات الفضاء السيبراني، وباستخدام منصات وتطبيقات برمجية محلية، مع استبعاد تام لجميع البرمجيات الوافدة للبلاد من الخارج.

ورغم الحرص الشديد لوزارة تقنية المعلومات والاتصالات على الالتزام بالبرنامج الزمني للمشروع، وسخاء الحكومة في توفير ميزانية ضخمة لتمويل المشروع بمبالغ ضخمة[60]، وتسخير جميع الطاقات الوطنية للتعجيل في عملية تنفيذ المشروع (*SMO,2014,b*)، وطلب الدعم التقني من دول صديقة، فلا زالت نسبة تقدم العمل بالمراحل الثلاث غير متداخلة وغير مكتملة، وبعيدة عن بلوغ البرنامج الزمني المعد مسبقاً لوصف تنفيذ فعاليات المشروع المختلفة.

فمن جهته، أبدى وكيل وزير تقنية المعلومات والاتصالات الإيراني، نصر الله جانكارد، بتصريح له في شهر تموز من عام 2015 شكوكه حول إمكانية بدء مشروع شبكة الانترنيت الوطنية وفق السقف الزمني الذي تبنته وزارته، عندما اكدت أن الشبكة ستباشر عملها في شهر مارس من عام 2016 القادم. وبرّر شكوكه في وجود تأخير كبير بتنفيذ الكثير من مراحل المشروع الحيوية، منها تراجع نسبة البيانات الداعمة لعمل الشبكة في المستودعات السيبرانية الوطنية، والتي لم تتجاوز لغاية هذا التاريخ 40%، رغم أن النسبة المستهدفة يجب ألا تقل عن 70-80% لضمان التشغيل الأولي للمشروع. وأضاف أن الإدارة الحكومية الإيرانية تروم امتلاك شبكة معلومات تهيمن الكوادر التقنية الإيرانية على إدارة جميع الأنشطة السيبرانية التي تسود فضاءها السيبراني، مع القدرة التامة على مراقبة جميع أشكال الخطاب الذي يسري في قنواتها السيبرانية المتعددة، وهو امر بعيد المنال وفق المعطيات التقنية ومستوى القدرات والخبرات التي تتمتع بها الكوادر التي تبذل قصارى جهدها لاستكمال هذه الشبكة العملاقة، بأهدافها وغاياتها.

[60] . ذكر محمد سليماني (وزير المعلومات والاتصالات السابق في حكومة أحمدي نجاد) أن الميزانية التي خصصت لعامي 2014-2015 هي الأكبر في تاريخ هذه الوزارة، وأن الهدف الأساسي للوزارة هو البدء بتشغيل شبكة الانترنيت الوطنية *SHOMA* خلال العام القادم (*SMO,2014,c*).

وتباينت ردود فعل الحكومة تجاه تأخر عملية تنفيذ المشروع، فقد استدعى البرلمان الإيراني وزير المعلومات والاتصالات الإيراني، فايزي، للوقوف على أسباب تأخر عمليات تنفيذ شبكة الانترنيت الوطنية *SHOMA*، في النصف الأول من عام 2015، بعد أن تكاثرت تصريحات المسؤولين الإيرانيين، وتناقضت توقيتاتها لبدء المشروع الذي يعده أعضاء البرلمان خطوة مهمة لدرء الهجمات التي تمارس من خلال نسيج شبكة الانترنيت على الكثير من مفاصل الدولة الإسلامية والشعب الإيراني (*SMO,2015,b*).

بالمقابل فقد تبادلت جهات متعددة الاتهامات بصدد تحديد أسباب التأخر الحاصل في تنفيذ مشروع شبكة الانترنيت الوطنية *SHOMA*. فقد أعلن خسرو سلجوقي (معاون رئيس مؤسسة تقنية المعلومات *ITO*) أن خطة مشروع شبكة الانترنيت الوطنية *SHOMA* قد اكتملت في النصف الأول من عام 2014، وعرضت على أنظار المجلس الأعلى لالفضاء السيبراني *SCC*، بالمقابل وجه محمد حسن انتظاري (سكرتير المجلس ذاته) انتقاداً لاذعاً لوزارة المعلومات والاتصالات بسبب اخفاقها في تقديم سقف زمني موضوعي لتنفيذ هذا المشروع الحيوي (*SMO,2014,c*).

ويمكن أن يبرر التأخير في عملية التنفيذ، الى أمور تقنية وتمويلية، ذلك لأن شبكة معلومات تلبي حاجات أكثر من خمسين مستخدم في إيران، مع عدد كبير من المؤسسات الحكومية، وشركات القطاع الخاص ليست شبكة تقليدية، وبحاجة الى خبرة تقنية متقدمة، إضافة الى التجاذبات المستمرة بين جهات تهيمن على القرار الحكومي (مثل الحرس الثوري الإيراني، والمجلس الأعلى للثورة الإسلامية في إيران، والمرجعية الدينية) ولا تمتلك دراية كافية بطبيعة الاحتياجات التقنية والتمويلية لتلبية مطالبها التي قد تتجاوز سقف الإمكانيات والقدرات التي تمتلكها الحكومة.

لذا وبالرغم من كثرة الوعود التي أطلقها الكثير من المسؤولين[61]، ومن مختلف مراتب الهرم الحكومي الإيراني، فقد تأجل موعد انطلاق خدمات شبكة الانترنيت الوطنية لأكثر من مرة خلال السنوات الأخيرة[62]. بيد أن الخطة الخمسية للتنمية الوطنية في إيران للسنوات 2011-2015 قد وضعت نصب عينيها الالتزام بتحديد نهاية الربع الأول من عام 2016 موعداً نهائياً لانطلاق شبكة الانترنيت المحلية، وبكامل طاقتها السيبرانية، وعلى عموم الرقعة الجغرافية لإيران (*ICHR,2014*).

5 . 3 . مصادر تمويل المشروع:

لقد اجبر الرئيس الإيراني حسن روحاني على الالتزام بمشروع شبكة الانترنيت الوطنية، بعد ان أصيبت جهوده بفشل ذريع، واضطر الى تغييب وعوده الانتخابية بصدد فتح أبواب فضاء الانترنيت للمواطن الإيراني بسبب تعدد مصادر الضغوط المعادية لخدمة الانترنيت التي تناسلت مواردها لدى مؤسسة الحرس الثوري، والتيار السياسية المحافظة، والمرجعيات الدينية التي ما انفكت توجه سهام الانتقاد نحو أي محاولة للتقليل من عتبة الحدود المفروضة على هذه الخدمة العدوانية.

---

61 . أكد نصر الله جهانكارد (وكيل وزير تقنية المعلومات والاتصالات) أن إدارته قد حرصت على توفير ثمان أدوات بحث لدعم عملية البحث والتصفح التي يمارسها المستخدم الإيراني عند إبحاره في الفضاء السيبراني، وأنه يأمل من الكوادر الوطنية بالمزيد من عمليات التطوير والتحسين على آلتي البحث *Yooz, Parsijo* بحيث يمكن القول أنهما سيتفوقان بالخدمات التي سيقدمونها للمستخدم الإيراني على ما تقدمه آلتي البحث *Google* و *Yahoo* .

62 . في نهاية شهر تموز 2015، ذكر نصر الله جهانكارد (وكيل وزير تقنية المعلومات والاتصالات) أن شبكة الانترنيت الوطنية *SHOMA* قد اكتملت وانها ستقوم بتوفير خدمة انترنيت مميزة للمواطنين الإيرانيين. وأضاف بأن وزارته ستنهض بمهمة إدارة المرور السيبراني في إيران، وتنوي ربط 60% من المساكن، و100% من المؤسسات الحكومية ضمن النسيج الشبكاتي لشبكة الانترنيت الوطنية.

فبذل ما في وسعه لتخصص ميزانية لتمويل مشروع شبكة الانترنيت الوطنية *SHOMA* وبتخصيصات تراوحت بين 4.5-3.75 مليار دولار لتعجيل عمليات استكمال إنشاء الشبكة وتشغيلها. بيد أن هذه التخصيصات لم تسعف محاولة روحاني في توقعت الحكومة الإيرانية أن يسهم تشغيل شبكة الانترنيت الوطنية في زيادة سرعة حزمة خدمة الانترنيت في إيران بمقدار 2.5 مرة، مع زيادة سرعة وصول المستخدم الى مواقع الويب التي تستضاف ضمن مضيفات الخدمة الموجودة في البلاد.

بيد أن هذه التخصيصات، غير المسبوقة[63]، لم تفي بمتطلبات تنفيذ شبكة الانترنيت الوطنية على أرض الواقع، بحيث أعلن وزير تقنية المعلومات والاتصالات في شهر تموز من عام 2014 أن مشروع شبكة الانترنيت الوطنية بحاجة الى تمويل إضافي يتراوح بين 1-1.5 مليون دولار بالإضافة الى الميزانية التي خصصت للمشروع وبلغت قيمتها (494 مليون دولار) (*SMO,2014,c*).

إن متابعة حفريات التخصيصات الحكومية لقطاع تقنية المعلومات والاتصالات في إيران خلال عقد من الزمان، تظهر بجلاء أن حصة هذه التقنيات واداوتها من الميزانية الإيرانية قد بدأت تزداد شيئاً فشيئاً. فارتفعت الميزانية بنسبة 95 % في بداية السنة المالية لعام 2014 فبلغت 1.36 مليار دولار (شكلت حوالي 1.55 % من الميزانية الكلية لإيران) بالمقارنة مع السنة السابقة[64]، كما أن الاقبال غير المسبوق للشعب الإيراني على استخدام هذه الأدوات في جل تفاصيل حياتهم اليومية، وتتنامي أنشطته الاتصالية والتواصلية قد أسهم في زيادة العوائد المالية بنسبة بلغت 18% وقاربت حوالي 1.92 مليار دولار (*SMO,2014,a*).

وتظهر قائمة مشاريع تقنيات المعلومات والاتصالات الجديدة، تراجع التخصيصات مشروع التجارة الالكترونية بنسبة 46 %، والشؤون الاستراتيجية لمشاريع المعلومات والاتصالات بنسبة 33 %، والبحوث التطبيقية بنسبة 28 %. اما الزيادة الكبيرة في حصص المشاريع الجديدة، فقد شملت خطط إدارة الحكومة الالكترونية بنسبة بلغت 607 %، ومشاريع تطوير المعايير والتنظيمات بنسبة 521 %، ومشاريع خطط أمن المعلومات بنسبة 325%، ومشروع حماية البيانات بنسبة 33 %.

وقد برر المركز البريطاني *Small Media Organization* المتخصص بمتابعة مشاريع البنية التحتية للمعلومات والاتصالات هذه الأمور المتناقضة بما يلي (*SMO,2014,a*):

- ☒ أن لدى وزارة تقنية المعلومات والاتصالات رغبة اكيدة في الإسراع بتنفيذ مشروع الحكومة الالكترونية، وتوسيع رقعة تطبيقاتها الداعمة لتقليص حجم الانفاقات الحكومية مع ضمان بيئة عمل آمنة ضد الاختراقات المحتملة لبيئتها البرمجية وتطبيقاتها.
- ☒ أسهم الاختراق الخطير الذي مارسه فايروس *Stuxnet* على منظومة أجهزة الطرد المركزي لمفاعل إيران النووي في تنامي القلق لدى وزارة تقنية المعلومات والاتصالات، وتركيز اهتمامها بمسألة أمن المعلومات، وحماية الأمن الوطني للمعلومات من جهات معادية تتربص لظهور أي ثغرة رقمية لكي تتسلل من خلالها الى مؤسسات الطاقة الذرية، والمؤسسات ذات الصلة بأنشطة الحرس الثوري والجيش ومؤسسات حكومية

[63] . ذكر محمد سليماني (وزير المعلومات والاتصالات السابق في حكومة أحمدي نجاد) أن الميزانية التي خصصت لعامي 2014-2015 هي الأكبر في تاريخ هذه الوزارة، وأن الهدف الأساسي للوزارة هو البدء بتشغيل شبكة الانترنيت الوطنية *SHOMA* خلال العام القادم (*SMO,2014,c*).

[64] . بلغت ميزانية عام 2014 ضعف ميزانية عام 2013، وثلاثة أضعاف ميزانية عام 2012 (*SMO,2014,a*).

مهمة. وقد أثمرت هذه الميزانية الضخمة في إصدار نسخة وطنية لمكافحة فايروسات الحاسب والكشف عن البرمجيات الخبيثة، بعد أن منيت المحاولات في سنين سابقة بالفشل.

- تؤشر الزيادة في ميزانية تطوير المعايير والتنظيمات الى رغبة الحكومة بتضييق الخناق في عملية حظر المراقبة، والمراقبة الذكية لمحتوى المواقع، وكف الأنشطة المناهضة لخطاطتها العقدية والسياسية.
- يبدو أن الوزارة ذاتها قد قللت من حجم اهتمامها بأنشطة البحوث والتخطيط الاستراتيجي الذي لم يعد يجدي نفعاً مع التغيرات المتسارعة بمضمار التحديات التي تواجهها في خضم فضاء الانترنيت.
- يلاحظ تقلص ملحوظ في ميزانية تطوير التجارة الالكترونية بسبب التنافس غير المتكافئ غير المتوازن مع أنشطة القطاع الخاص، والتي اثبتت قدرتها على التفوق بجدارة على ممارسات الحكومة، فتركت مسألة التطوير للقطاع الخاص، ووفرت تخصيصات القطاع لأنشطة أخرى تخص القطاع الحكومي.

من جهة أخرى يلاحظ أن ارتفاع قيمة ميزانية مشاريع تقنية المعلومات والاتصالات لم توزع بصورة متكافئة، حيث إن حصة الميزانية التخطيطية للإنفاقات *Planned Expenditure Budget (PEB)* قد تراجعت بنسبة 22 % بينما قابلها ارتفاع مناظر في حصة الميزانية التخطيطية- المتنوعة *Planned Miscellaneous Budget (PMB* وبمعدلات غير مسبوقة. ويؤشر هذا التناقض الى تناقص نسبة المشاريع الجديدة التي تقع ضمن دائرة مسؤولية وزارة تقنية المعلومات والاتصالات، وتزايد مشاريع تقنيات المعلومات والاتصالات التي لم يتخذ قرار حاسم بصدد الجهة ستكلف برعايتها، سواء من قبل مؤسسات القطاع الحكومي، أو بعض شركات القطاع الخاص.

ويمكن أن يعزى هذا الأمر الى رغبة حكومة روحاني بتوفير مرونة كافية في التعامل مع الميزانية بعيداً عن هيئة البرلمان الإيراني الذي قد يبدي الكثير من الاعتراضات على المشاريع التي تسهم بتطوير سعة خدمة الانترنيت، وسرعتها. كذلك فإن إلحاق مشروع الانترنيت الوطني بمشاريع الميزانية المتنوعة، وعدم اتضاح حجم الانفاقات المطلوبة لتنفيذه، وإلحاح المؤسسة الدينية والحرس الثوري على الإسراع بإكمال المشروع، قد ألجأ الحكومة الى توفير نسبة كبيرة من التخصيص لتغطية الحاجة الطارئة التي يتطلبها تنفيذ مشروع لم تتضح معالمه، وتتنازع في تحديد خصائصه جهات عقدية وسياسية قبالة مؤسسات تقنية وطنية قد لا ترقى خبراتها الى مستوى تحقيق هذا الحلم الوطني.

وبالوقت ذاته، فإن المثير للاهتمام أن تمويل شركة الانترنيت الوطنية *SHOMA* قد خصص من ميزانية *PMB* الأمر الذي سيمنح حكومة روحاني حرية التصرف في مسارات تطوير الشبكة، مع تأخير قرار حكومته باختيار هوية الوزارات الحكومية وشركات القطاع الخاص التي ستعمل ضمن فريق تنفيذ المشروع الوطني للانترنيت البديلة .(*SMO,2015,c*)

5 . 4 . الدعم التقني من دول صديقة:

سعت إيران الى كسب تعاطف ودعم لمشروعها، من دول صديقة، تشترك معها بمعاداة الفضاء المفتوح الذي جاءت به شبكة الانترنيت، وتطبيقات منصات التواصل الاجتماعي التي وفرت فضاءَ تواصلياً مفتوحاً امام المستخدمين. وقد نجحت في مد جسور التعاون مع كل من الصين وكوريا الشمالية في مجالات حظر المواقع، وتقطير المحتوى، ثم طلب الدعم لاستكمال مشروع شبكة الانترنيت الوطنية.

وقد حاولت الحكومة الى زج القطاع الخاص الإيراني في مشروع إنشاء شبكة SHOMA لتوفير مناخ تنافسي في البلاد قادر على جذب المواطنين الى خدمة الانترنيت الوطنية، وللتقليل من حجم الميزانية المطلوبة لتنفيذ المشروع من خلال جذب الشركات المحلية للاستثمار بقطاع تقنية المعلومات.

فقد عمد وزير تقنية المعلومات والاتصالات، محمد فايزي، الى اصطحاب مجموعة مجموعة من رجال الأعمال الإيرانيين، مع مدراء كل من: شركة اتصالات إيران، وشركة *Irancell* وشركة *Rightel*، وشركة الشبكة الإيرانية *Iranian Net*، في زيارة عمل للقاء وزير الاتصالات الصيني في 8 يونيو عام 2015 للدخول في مباحثات تقنية، وترسيخ التعاون بين الشركات الإيرانية وشركات صينية، مع معاودة الطلب لتوفير الدعم التقني لتعجيل عملية تنفيذ مشروع شبكة الانترنيت الوطنية *SHOMA*.

وقد صرّح الوزير الإيراني، بعد استكمال مهمة الوفد، بأن الجانب الصيني سيشارك في تطوير شبكة البيانات الوطنية، مع قيام الطرفين بتوقيع اتفاقية مشتركة للتعاون على صعيد محاربة القرصنة والهجمات السيبرانية التي تتعرض لها مواقع البلدين داخل حدود الفضاء السيبراني (*SMO,2015,b*). ورغم أن الوزير الإيراني لم يفصح يصفح عن طبيعة وتفاصيل عملية الدعم التي ستوفرها الصين لإيران في هذا المجال. بيد أن قصور خبرة الجانب الإيراني في مجال تقنية المعلومات، قبالة التقدم الذي بلغته الصين في هذا المجال، يؤكد وجود رغبة أكيدة لدى الجانب الإيراني في محاكاة الأنموذج الصيني لشبكة المعلومات البديلة للانترنيت، مع إضافة لمسات بسيطة تحاول أن تصبغ شبكة *SHOMA* بصبغة ظاهرية توحي بأن هوية الشبكة إيرانية صرفة.

الفصل الثالث:
دور الحكومة الإيرانية في حوكمة وإدارة الفضاء السيبراني

الفصل الثالث: دور الحكومة الإيرانية في حوكمة وإدارة الفضاء السيبراني

1 . الاستراتيجية السيبرانية ـ الإيرانية:

احتلت أدوات الاتصالات مكانة بارزة لدى المؤسسة الإيرانية، منذ عهد الشاه، حيث خصصت ميزانية ضخمة لتوطين تقنيات الاتصالات الحديثة قبل عام 1979، مما جعل إيران تتفوق بهذا المجال على الكثير من بلدان الشرق الأوسط. غير أن الاعصار الذي جاءت به الثورة الإسلامية قد اورث حكومتها المحافظة انشغالات جديدة تركزت باتجاه توطيد أركان الثورة ونشر ثقافتها، فخفت بريق أدوات المعلومات والاتصالات من مشهد التنمية في إيران، بعد أن اشتعلت نار حرب الخليج ودخلت البلاد في دوامة حرب ضروس مع العراق، في بداية عقد الثمانينات من القرن العشرين، فغيّرت الكثير من معالم خطط التنمية الوطنية التي حوّلت جل ميزانيتها لتوفير آلة للدفاع عن حياض إيران وحماية بيضة ثورتها الإسلامية الوليدة (*Soofi&Ghazinoory,2013*).

ومع انجلاء غبار حرب الثمان سنوات، وعودة الحياة الطبيعية، شيئاً فشيئاً، الى المشهد الإيراني، عاودت النخبة التقنية الإيرانية بالضغط على الحكومة لمعاودة برنامج تنمية وتطوير البنية التحتية للمعلومات والاتصالات في إيران، لتعويض ما فاتها خلال سنوات الحرب، وإعادة المكانة التي تمتعت بها إيران بالمضمار تقنية المعلومات والاتصالات. وجدت نداءات النخبة التقنية استجابة سريعة، عندما اقتصرت الأنشطة الاتصالية على خطوط الهواتف الأرضية، بيد ان ولادة تقنية فضاء الانترنيت، والهواتف المحمولة قد اثارت المزيد من القلق لدى الإدارة الحكومية بعد أن تعالت أصوات المحافظين من المجلس الإيراني، والمؤسسات العسكرية والأمنية التي استشعرت وجود تهديدات محتملة من خارج غيران، مع توفر مناخ مناسب لإيقاظ الأصوات المناهضة لخطاب الثورة الإسلامية من داخل حدود إيران. فتأرجحت استراتيجية الحكومة الإيرانية بين توسيع قاعدة الاتصالات والمعلومات من جهة، مع تضييق الخناق على فضاء التواصل والاتصالات، من جهة أخرى، فأصيبت الاستراتيجية بتشوهات متعددة نتيجة التناقض بين الخطاب التقني، والخطاب السياسي، بمختلف تجلياته، مما وسم الاستراتيجية السيبرانية الإيرانية بصبغة فريدة تتنازعها نكهة تقنية اصطنعت في دائرة النخب التقنية، ونكهة محافظة مصدرها قيادات المجلس الأعلى للثورة الإسلامية، والحرس الثوري الإيراني، وجهات أخرى.

وقد تغلبت الصبغة المحافظة على بقية النداءات التي أطلقها التنويريون فصبغت الاستراتيجية بصبغتها المحافظة، والتي ترجح لديها كفة إبطاء سرعة الخدمة، وتفعيل برامج الحظر والمراقبة، حتى نهاية الولاية الثانية لمحمود أحمدي نجاد، بينما بدا الانفراج الجزئي مع ولاية الرئيس حسن روحاني، إلا أن عملية التغيير لا زالت في بداياتها، ولا زالت بحاجة الى زمن ليس بالقصير لإنجاح عملية التحول نحو فضاء معلومات توجه دفته النخب التقنية بعيداً عن عصابات القيادات الأمنية وهواجسها غير المتوازنة في عصر الانفتاح السيبراني المعاصر.

ونظراً للاهتمام المتزايد بتوطين أدوات المعلومات والاتصالات في البيئة الإيرانية، ووجود رغبة في استثمار تطبيقاتها لتحقيق قفزة كبيرة على صعيد بلوغ أهداف الإدارة الحكومية فقد فوضت الحكومة وزارة تقنية المعلومات والاتصالات لتوقيع اتفاقية مع مؤسسة الإدارة والميزانية (*MBO*) *Management & Budget Organization* لصياغة خطة شاملة لتنمية وتطوير تقنية المعلومات بالبلاد ومن خلال خمسة مشاريع استراتيجية. شملت هذه المشاريع (*Soofi&Ghazinoory,2013*):

- ✓ مشروع إعداد خطة شاملة لتوسيع انتشار تقنية المعلومات والاتصالات، أدوات وتطبيقات.

- ✓ مشروع إعداد وصف وظيفي للمهام والمسؤوليات المنوطة بوزارة تقنية المعلومات والاتصالات على صعيد ملف الأمن السيبراني الوطني.
- ✓ إنشاء وتطوير قاعدة بيانات تضم احصائيات تفصيلية عن كيفية متابعة وضمان تنفيذ المشاريع على أرض الواقع.
- ✓ إعداد إطار عام لخطة تطوير تطبيقات وطنية في مجال تقنية المعلومات والاتصالات.
- ✓ إعداد مسودة مشاريع قوانين وتنظيمات لمراقبة وإدارة الأنشطة السائدة في الفضاء السيبراني الوطني.

1 . 1 . مشروع البرنامج الوطني الإيراني لقطاع تقنية المعلومات والاتصالات:

قام المجلس الأعلى لتقنية المعلومات والاتصالات (بوصفه الجهة العليا المسؤولة عن اتخاذ القرارات وصياغة السياسات ذات الصلة بتقنيات المعلومات والاتصالات بإيران) *Supreme Council of Information & Communication Technology (SCICT)* بتنفيذ امر رئيس الجمهورية بصدد إعداد خطط تفصيلية لتنمية قطاع الاتصالات والمعلومات بالبلاد خلال السنوات 1999-2002. وقد حشد المجلس طيفاً عريضاً من الطاقات الوطنية بقطاع التخطيط لغرض إعداد خطة وطنية طموحة، بعد الاطلاع على خطط أعدت في بلدان أخرى نجحت في تمثّل وتوطين تقنية المعلومات بنجاح على المستوى الوطني (*Jahangard,2004*). وقد شاع إطلاق اصطلاح *TAFKA* على هذه المبادرة الوطنية، والذي يعبر باللغة الفارسية عن برنامج وطني يعنى تطوير قطاع تقنية المعلومات والاتصالات.

ارتكزت خطاطة المشروع الجديد الى وجود قناعة أكيدة لدى الإدارة الإيرانية بضرورة إجراء دراسة تفصيلية لأسباب نجاح الاستراتيجيات الوطنية التي تبنتها دول في المنطقة، ودول متقدمة، ثبت نجاها على أرض الواقع، لغرض استثمارها في صياغة استراتيجية وطنية، رشيدة، قادرة على تحديد مواطن الضعف، وعناصر القوة التي تتسم بها البيئة الإيرانية ولكي تكون الاستراتيجية أكثر قرباً من واقع البلاد، مع ضمان نجاعتها في تحقيق الأهداف المرسومة لها (*Davarinejad&Saffari,2010*).

وقد أرادت النخب التقنية تشكيل هيكلة مؤسسية تتسم بالمرونة، وقادرة على إدارة المهام المعقدة، والمتشابكة، لمشروع معلوماتي طموح، يحاول ان يحقق طفرة بالبلاد، تدعمه إدارة مالية تمتلك آلة اقتصادية مقتدرة، وغير تقليدية، تمتلك معرفة عميقة بحجم الميزانية التي يتطلبها تنفيذ مشروع سيحضن الاستراتيجية الإيرانية السيبرانية، مع ضمان عدم حصول أي قصور في حجم التخصيصات أو توقيتاتها، بحيث ينعكس سلباً على السقف الزمني المخطط لتنفيذ المشروع.

بيد أن واقع المشهد السياسي الإيراني، المشحون بحضور مراكز قوى متعددة، تتجاذب فيما بينها في تنازع السلطة على إنتاج الخطاب الموجه لجميع تفاصيل المشهد الإيراني، قد اورث المشروع مسارات جديدة لتوجيه رؤى ومهام مشروع *TAFKA*، فأصبحت الرؤية الوطنية للمشروع محكومة بتوجيهات المرشد الأعلى للثورة الإسلامية، بالمرتبة الأولى، ثم بطبيعة الأولويات التي يحددها رئيس الجمهورية، بالمرتبة الثانية، واخيراً بالإطار العام الذي يحدده المجلس الأعلى لتقنية المعلومات والاتصالات في إيران (*Jahangard,2004*).

لذا كان لا بد للرؤية التي اصطنعت في أروقة المعرفة التقنية أن تنصاع لرؤية ثلاثية، الرؤية العقدية التي تتحدد معالمها لدى المرشد الأعلى، والرؤية السياسية التي تفرضها الإدارة الحكومية، وطبيعة الإطار الذي يفرضه مجلس تتقاسم مقاعده مجاميع متعددة من القيادات المعلنة وغير المعلنة والمسؤولة عن إدارة أجزاء متعددة من دفة

النظام الإيراني. وستكون النتيجة النهائية عبارة عن مزيج غير متجانس من الآراء التي تنتمي الى خطاطات متباينة، ويصعب بلوغ توافق تام في مزيجها المتناقض.

وقد تولّدت في رحم هذه التجاذبات خطاطة مشروع *TAFKA* والتي ارتكزت الى خمسة محاور أساسية (*Jahangard,2004*):

المحور الأول: البنية التحتية:

حيث سيتوجه اهتمامه نحو فرص الوصول الى موارد المعلومات، وضمان توفير بيئة آمنة لحفظ المعلومات وتداولها، وإنشاء مراكز البيانات في عموم البلاد، وصياغة قواعد تنظيمية وقوانين تحكم عمليات الدخول، وتداول المعلومات، والحفاظ على أمنها، وكف عمليات التجاوز على المحتوى أو سرقته.

المحور الثاني: الخدمات الاقتصادية والتجارية:

ويعنى بنشر وتطوير أنشطة التجارة الالكترونية، وتعاملات المصارف السيبرانية، واستخدام النقود الالكترونية داخل حدود بيئة آمنة، وقادرة على كسب رجال المال والأعمال لممارسة انشطتهم في فضائها الآمن.

المحور الثالث: الخدمات الحكومية:

والذي سيوجه اهتمامه نحو الخدمات الالكترونية التي توفرها الحكومة للمواطن الإيراني، وخدمات الحكومة الالكترونية، مع بسط سلطان حوكمة الإدارة الحكومية الإيرانية على الفضاء السيبراني والاتصالات بالبلاد.

المحور الرابع: تطوير الموارد البشرية ورعاية برامج التنمية الثقافية والاجتماعية:

والتي ستوجه عنايتها نحو بناء القدرات السيبرانية والتواصلية لدى الموارد البشرية الوطنية، وتعزيز برامج التعليم الالكتروني، والتعلّم عن بعد، وتوطين الخطاب الثقافي الإيراني في البيئة السيبرانية مع إثراء المحتوى السيبراني ـ الفارسي.

المحور الخامس: التوظيف والصناعة:

وقد خطط لهذا المحور أن يساهم في تطوير الآلة الصناعية الإيرانية من خلال توطين التقنية السيبرانية في حظيرة الصناعة الوطنية، مع توفير فرص عمل للموارد البشرية العارفة، ونشر حواضن الابتكار في مجال التقنية السيبرانية، مع دعم الشركات الصغيرة والمتوسطة التي تتخصص لتوفير قاعدة داعمة للبيئة الاتصالية الوطنية، وبمختلف مجالات احتياجاتها على أرض الواقع.

وقد تضمنت وثيقة هذه الاستراتيجية الدعوة الى الإسراع في عملية ردم الفجوة بين واقع تقنية المعلومات بإيران، وما بلغته الدول الصناعية المتقدمة بهذا المجال الحيوي من خلال: تطوير وتعميق جذور، أنموذج وطني، يرتكز الى المتغير المعرفي لضمان الالتحاق بركب مجتمعات المعلومات والمعرفة المعاصرة. واقترحت بلوغ هذا الهدف من خلال توطين المزيد من التقنيات والسلع السيبرانية من البلدان المتقدمة، ومحاولة استنبات منتجات وتطبيقات معرفية بواسطة الكوادر الإيرانية تلبي الحاجات المتزايدة للدولة الإسلامية، وترسّخ جذور تفوقها على صعيد التقنية السيبرانية بالمنطقة[65] (*Soofi&Ghazinoory,2013*).

وضم مشروع *TAKFA* أكثر من 110 مشروع أساسي لدعم برامجه التطويرية، تضمنت هذه المشاريع أكثر من 5,000 مشروع ثانوي توزعت على جميع قطاعات الأنشطة السيبرانية والاتصالية بالبلاد. بيد ان تشتت خطاطة هذه المشاريع لتلبية مجموعة متناقضة من المطالب التي صدرت عن المؤسسة الأمنية، والمرجعيات، والمجلس، اورث

[65] . تبنت الخطة شعاراً دعا الى: توليد فرص مناسبة لوصول جميع طبقات المجتمع الإيراني الى تقنيات السيبرانية، والتدريب الشامل للموارد البشرية بحيث توظف هذه التقنيات في جميع مفاصل الحياة اليومية، وإنشاء بيئة حاضنة لجميع أشكال الابتكار وتوسيع نطاق الشبكات الذكية في نسيج المعلومات الإيراني لضمان إحداث تغييرات حاسمة في أنموذج التطور المعرفي بالبلاد، وتجاوز عقبة الفجوة السيبرانية التي تفصل إيران عن مجتمعات المعلومات والمعرفة العولمية.

المشروع عدداً كبيراً من المشاريع التي بوشر بالعمل عليها، دون وجود بادرة في الأفق لاكتمالها، أو استمرار العمل عليها؟، الأمر الذي تسبب في نهاية هذا المشروع في عام 2005، ليلد محله في عام 2006 مشروع جديد أطلق عليه *TASMA* وأضحى يعرف بالمرحلة الثانية *TAKFA2*.

وعاودت إدارة مشروع *TASMA* الى وضع أهداف جديدة للاستراتيجية الوطنية تمثلت بتوجيه اهتمامها الى الأهداف التالية (*Davarinejad&Saffari,2010*):

- ✓ تطوير خدمات الحكومة الالكترونية.
- ✓ الاهتمام بالتعليم وبناء القدرات، وتطوير المهارات السيبرانية.
- ✓ تبني برامج متنوعة لتطوير قطاع التعليم العالي، والصحة، والتشخيص الطبي، والتدريب.
- ✓ تطوير وتوسيع دائرة الخدمات السيبرانية.
- ✓ تطوير بيئة التجارة الالكترونية وجذب القطاع الخاص نحو الفضاء السيبراني.
- ✓ الاهتمام بتطوير المحتوى السيبراني الإيراني، وتوسيع دائرة استخدام اللغة الفارسية في بيئة الحاسب وتطبيقاته المختلفة.
- ✓ توفير الدعم اللوجستي، وجذب الاستثمارات المحلية والأجنبية لقطاع الصناعات السيبرانية لتنشيط قطاع الصناعات الصغيرة والمتوسطة في البلاد لتلبية الاحتياجات المتزايدة للسوق الإيرانية من أدوات المعلومات والاتصالات وخدماتها المختلفة.

وبقي مشروع *TASMA* مقيداً بغياب الدعم الحكومي الكافي، وشحة التخصيصات المالية لتمويل المشروع، وتراجع جاهزية البنية التحتية للمعلومات والاتصالات مع ارتفاع كلف خدمة الانترنيت وتباطؤ سرعتها مما وقف عائقاً امام تنفيذ الكثير من المشاريع التي تفتقر الى هذه الموارد السيبرانية، وغياب اللغة المشتركة بين القطاع الحكومي والقطاع الخاص بصدد تنشيط الاستثمار بقطاع الاتصالات والمعلومات واحتكار بعض المؤسسات الحكومية وهيمنتها على سوق المعلومات والاتصالات، مع وجود التجاذبات لدى الجهات المسؤولة عن صناعة القرار، وتغير الأولويات بحسب قناعات تصاغ مادتها خارج حدود مؤسسات تقنيات السيبراني والاتصالات ذات الصبغة المهنية، فتتناقض الأهداف، وتتعارض المشاريع، وتعاد صياغة الأهداف مما أفقد المبادرة الأهداف التي اقترحت من اجلها (*Davarinejad&Saffari,2010*).

1 . 2 . الجهات التي تعمل على إعداد الاستراتيجية الإيرانية:

بصورة عامة تتقاسم مهمة إعداد الاستراتيجية والسياسات الوطنية في قطاع المعلومات والاتصالات جهات متعددة من هرم مؤسسات الإدارة الحكومية بإيران (*Abbasi., et.,al.,2008*). فتنحصر مسؤولية وزارة تقنية المعلومات والاتصالات بالمفردات ذات الصلة بالتنمية الوطنية لهذا القطاع بعموم البلاد. وينصب اهتمام مجلس التميز لتقنية المعلومات *Information Technology Council Excellence* (*ITCE*) على صناعة القرارات الاستراتيجية، على المستوى الوطني، وصياغة سياسات تقنية المعلومات.

ويوجه مركز إيران لبحوث الاتصالات *Iran Telecom Research Center* (*ITRC*) جل اهتماماته على صعيد رسم سياسات واستراتيجية توسيع دائرة البحوث وتشجيع إنتاج المادة المعرفية، وتوفير المناخ المناسب للأنشطة الاستشارية التقنية ذات الصلة بتطوير تقنية المعلومات في إيران.

بينما اوكلت مهمة تقييم وتحديد مراتبية شركات الحواسب الى المجلس الأعلى لمعالجة البيانات *High Council of Data Processing* (*HCDP*).

أما بالنسبة لإعداد وثيقة مشروع البرنامج الوطني الإيراني لقطاع المعلومات *TAKFA* فقد شكلت تسع لجان من المتخصصين بمضمار تقنية المعلومات، وخبراء في مجال إعداد الاستراتيجيات السيبرانية، وآخرين من المتخصصين بمجال الإدارة وإعداد الخطط من القطاعين الأكاديمي والبحثي لإعداد مسودة وثيقة الاستراتيجية العامة لنظام تقنية المعلومات في إيران.

بذلت جهود كبيرة من قبل فريق العمل، واستغرقت منهم عملية إعداد هذه الوثيقة أكثر من 21,000 ساعة من العمل، ولاقت الوثيقة قبولاً من الإدارة الحكومية وصودقت من قبل أعضاء الكابينة الرئاسية في 26 ديسمبر من عام 2007 (*Soofi&Ghazinoory,2013*).

1 . 3 . حصة تقنية المعلومات والاتصالات في الخطط التنموية الخمسية:

مع نهاية الحرب العراقية ـ الإيرانية توجهت الحكومة الإيرانية الى اعتماد مبدأ الخطط التنموية الخمسية *FYDP*، للتخطيط الاقتصادي على المستوى المتوسط *Medium-Term Plans*. وتعد الخطط الخمسية، الثالثة، والرابعة، والخامسة، من أكثر الخطط التنموية ذات الأثر الملموس على تطوير قطاع الاتصالات والمعلومات في التاريخ المعاصر لإيران (*Ghasimi,2012*).

تبنت الخطة الخمسية الثالثة شعار خصخصة قطاع الاتصالات والمعلومات من خلال طرحها لثلاثة محاور، شكّلت مادتها معالم الخطة الاستراتيجية المنشودة. وتضمنت هذه المحاور: زيادة مساحة التغطية للخدمات السيبرانية والاتصالية، مع الارتقاء بجودة الخدمة؛ وإصدار تراخيص للقطاع الخاص في إيران لنشر خدمات الهواتف الأرضية والمحمولة، وتناقل البيانات بواسطة حزم المعلومات العريضة، والخدمات اللاسلكية؛ وتشكيل هيئة تنظيمية تنهض بمهمة تنفيذ تفاصيل الاستراتيجية وسياساتها التفصيلية، مع القيام بمهمة إرشاد القطاع الخاص للالتزام بتوقيتات برامج الخطة (*Davarinejad&Saffari,2010*).

من جهة أخرى، صادق المجلس الإيراني على قانون الخطة التنموية الخمسية ـ الرابعة، والتي أرادت الحكومة الإيرانية لها أن تمهّد الطريق أمام نهضة وطنية بمضمار الاقتصاد المرتكز الى المعرفة، بحيث تدعم عملية انتقال الاقتصاد الإيراني والتحاقه وتفاعله مع الاقتصاد العولمي الجديد (*MPO,2005*).

وجهت الخطة التنموية الخمسية (الرابعة) للسنوات (2005-2009) اهتمامها نحو زيادة أعداد مستخدمي الهواتف الأرضية، والانترنيت والهواتف المحمولة. وبلغت ميزانية مشاريع المعلومات والاتصالات خلال مدة الخطة الخمسية حوالي 25 مليار دولار، خصص 19 مليار دولار منها لمشاريع تنمية البنية التحتية الاتصالية، بينما خصص مبلغ 6 مليارات دولار لمنصات تقنية المعلومات وبنيتها التحتية الداعمة (*Abbasi., et.,al.,2008*).

وتضمنت الاستراتيجية الوطنية ـ الشاملة مجموعة من المحاور التي عنيت بتطوير البيئة السيبرانية في إيران من خلال تفعيل مجموعة من الاستراتيجيات الثانوية التالية (*Abbasi., et.,al.,2008*):

- ✓ الاستراتيجية الوطنية لتطوير تقنيات وأدوات المعلومات والاتصالات، ووثيقة سياسة تقنية المعلومات.
- ✓ الاستراتيجية الوطنية لتقنية المعلومات التي تعنى بالخدمات الالكترونية، والتي شملت خدمات: الحكومة الالكترونية، والتجارة الالكترونية، والتعليم الالكتروني، والصحة الالكترونية.
- ✓ خطة خصخصة قطاع الاتصالات.

- ✓ خطة تحويل شبكة الاتصالات من الشبكة التقليدية باتجاه شبكة الجيل الجديد *NGN*.
- ✓ التحوّل من احتكار الحكومة لقطاع الاتصالات باتجاه بيئة تنافسية مفتوحة.
- ✓ جذب وتشجيع الاستثمارات الأجنبية في قطاعات المعلومات والاتصالات.

وفي الوقت ذاته خصصت الحكومة 2% من الميزانية الوطنية لتمويل أنشطة البحث والابتكار في قطاع تقنية المعلومات لتوفير بيئة وطنية حاضنة لصناعات صغيرة وأخرى متوسطة تلبي الاحتياجات المتزايدة للسوق الاتصالية المحلية لسلع وخدمات معلوماتية، وبرمجيات توسع من دائرة حضور التقنيات السيبرانية والاتصالية في جل تفاصيل حياة المواطن الإيراني.

وفي تلك الحقبة، استأثر مركز إيران لبحوث الاتصالات *ITRC* بعملية إعداد وتطوير مادة الاستراتيجية الوطنية لتقنية المعلومات، وعكفت كوادره على إعداد خطة التحول باتجاه شبكة الاتصالات الجديدة *NGN*. أما مناخ حضانة ودعم الصناعات الصغيرة والمتوسطة، فقد وفرته مجموعة حدائق وحاضنات الابتكار التي أنشأتها الحكومة للنهوض بهذه المهمة، نذكر منها: حديقة طهران للبرمجيات والمعلومات والتقنية *Tehran Software & Information Technology Park*، وحديقة تقنية المعلومات التابعة للمركز الإقليمي للتميز في قطاع المعلومات والاتصالات *Regional Center of Excellence of ICT (RCEICT)*، بالإضافة الى حاضنات تقنية وحدائق تقنية أنشأت في محافظات أخرى.

وقد ساهمت هذه الحاضنات والحدائق التقنية بتوفير دعم تقني وبذل مشورة علمية واقتصادية لرعاية الصناعات الصغيرة والمتوسطة، وضمان سيرها على طريق سليم بدعم مباشر من الخبراء والأكاديميين في مراكز البحوث الوطنية، والقطاع الأكاديمي، وبالتنسيق مع شركات وطنية ومستثمرين لتغذية المشاريع بموارد اقتصادية تساعدها على تحقيق عوائد مالية مضافة تسهم بنجاحها وترسيخ حضورها في سوق الاتصالات والمعلومات الإيراني.

ولم تمر سوى بضع سنوات حتى التحقت بالاستراتيجية العامة، الاستراتيجية التي تضمنتها الخطة التنموية الخمسية (الخامسة) للسنوات (2011-2016) والتي خصص جزء من ميزانيتها لتنمية وتطوير قطاع المعلومات والاتصالات من خلال:

- ✓ إنشاء قواعد بيانات لملفات الرعاية الصحية الالكترونية للمواطنين الإيرانيين.
- ✓ توفير خدمات تأمين صحي يتكامل أداؤها مع قواعد بيانات الرعاية الصحية الالكترونية.
- ✓ توسيع نطاق شبكة الوطنية للمعلومات *SHOMA*.
- ✓ طرح المزيد من الخدمات الحكومية عبر منافذ وبوابات الحكومة الالكترونية.
- ✓ تطوير محتوى والخدمات التي توفرها البطاقة الوطنية الذكية للمواطن الإيراني.
- ✓ توسيع نطاق البيانات المكانية الوطنية من خلال زج تطبيقات نظم المعلومات الجغرافية وربط بياناتها بمنظومة طبقات خدمات البنية التحتية.
- ✓ إنشاء قواعد بيانات متكاملة تغطي المسائل القانونية ذات الصلة بقطاع العقارات، ودعمها بنظام معلوماتي آمن لتداول البيانات ضمن شبكة المعلومات الوطنية.
- ✓ دعم برامج ومشاريع إنشاء نظم معلومات للمشاركة بموارد المعلومات، وتكامل عناصر مستودعات البيانات بين مؤسسات الدولة المختلفة لبلوغ مرتبة متقدمة على صعيد حوكمة موارد الإدارة الحكومية.

- ✓ الاستمرار بتوسيع نطاق البنية التحتية الداعمة لشبكات البحث العلمي والتنمية الوطنية.
- ✓ ترسيخ الثقة بمتعاملات التجارة الالكترونية من خلال استكمال تعريف نطاق الشهادات الالكترونية، والتطبيقات الداعمة لهذا النشاط الحيوي.
- ✓ توسيع نطاق أنشطة المصارف الالكترونية، وإشاعة استخدام نظام التوقيع الالكتروني، والتواصل المصرفي عن بعد *Telecommuting Banking -Services*.

كما تضمنت فقرات الخطة الخمسية، بدورتها الخامسة التأكيد على مسائل أخرى منها: تشجيع صناعة محتوى رقمي رصين يعكس عمق الثقافة الإسلامية الإيرانية، وتوجيه الاهتمام بالعلم والتقنية، ومسائل ذات صلة بتطوير ورقمنة أنشطة المجتمع الإيراني (الضمان الاجتماعي، والخدمات الاجتماعية الداعمة، والصحة العامة)، وتطوير أنشطة الإدارة الالكترونية، وترسيخ إجراءات الإصلاح الاقتصادي بما يتوافق مع متطلبات الاقتصاد السيبراني سواء في مجال نظم الضرائب، وأسواق رأس المال، وتحسين سوق العمل، والأنشطة المالية والمصرفية. وقد أولت عناية خاصة بالمسائل ذات الصلة بأمن المعلومات الوطني، وحماية النسيج الشبكاتي من محاولات الاختراق وإحداث الضرر بمؤسسات الدولة الأمنية والتقنية، ولم يغب عن برامجها مشاريع رقمية لتطوير أداء المنظومة القانونية والتشريعية، ونظم الرقابة المالية والإدارية.

وعلى صعيد آخر، شملت قائمة تحقيق الأهداف التنموية لخطط تنمية المعلومات التي تبنتها الإدارة الحكومية الإيرانية، مع نهاية عام 2015، رسم الأهداف المدرجة في الجدول (3 - 1).

الجدول (3 - 1) ـ أهداف استراتيجية المعلومات الإيرانية لعام 2015.

القطاع	الهدف المنشود
تطوير التعليم الالكتروني.	30 %
تطوير التجارة الالكترونية.	20 % المستوى المحلي 30 % المستوى الدولي
نسبة تصدير تطبيقات برمجية وخدمات معلوماتية.	1.5 % من حصة التصدير غير النفطي
حصة برمجيات وتطبيقات أمن المعلومات.	2 % من الناتج الإجمالي المحلي
تغطية المساكن بخدمة الانترنيت العريضة.	60 %
توفير خدمات حكومة ـ حكومة *G2G*.	100 %
توفير خدمات حكومة ـ مواطن **G2C** وخدمات حكومة ـ تجارة وأعمال G2B.	70 %
استبدال التعاملات النقدية بالتسديد الالكتروني.	80 %
إكمال وثائق الصحة الالكترونية للمواطنين.	100 %
إكمال البطاقة الوطنية الذكية للمواطن.	100 %

المصدر: *ITU,2013*.

ولا زالت التقارير الحكومية تقرّ وجود تأخير في جل فقرات الخطة المنشودة لاستراتيجية المعلومات الإيرانية بسبب آثار الحصار الاقتصادي من جهة، وكثرة وضخامة حجم المهام التي أوكلت للجان التقنية العاملة على مشاريع متعددة، وبمجال يتجاوز الى حد كبير حجم الخبرات التي تمتلك الموارد البشرية الوطنية، أو تلبيها التخصيصات المالية بالوقت ذاته.

2 . معمارية مؤسسات تقنيات المعلومات والاتصالات بإيران:

انصبغت الهيكلة المؤسساتية، لقطاع المعلومات والاتصالات في إيران، بالصبغة ذاتها التي تميزت بها المؤسسات السياسية الإيرانية، وهي صبغة التعددية، وتداخل المهام، وتكاثر الجهات التي تصنع قراراتها. وقد برزت هذه الظاهرة نتيجة للتجاذبات المستمرة بين مراكز القوى المتعددة في البلاد، والتغير المستمر في مواقف القائد الأعلى للثورة الإسلامية، ومؤسسة الحرس الثوري الإيراني، وأعضاء المجلس، ومراجع الحوزات العلمية تجاه الفضاء السيبراني والاتصالات، فانعكست آثار هذه الظاهرة على استمرار عمليات إعادة الهيكلة للمؤسسات التي تعمل في قطاع المعلومات والاتصالات، واقتراح هيئات ومجالس جديدة، وإلغاء أخرى، وإعادة توزيع المسؤوليات، وتقاسم السلطات.

ورغم التغييرات المستمرة في معمارية مؤسسات المعلومات والاتصالات بإيران، منذ عام 2009، واستحداث وحدات تنظيمية جديدة، وتعليق عمل أخرى، إلا أنه يمكن تبويب مكونات هذه المعمارية الى ثلاثة طبقات تتكامل في أدائها لإدارة ملف المعلومات والاتصالات بعموم البلاد (*FWC,2014*):

الطبقة العليا: المجالس العليا والهيئات:

وتتضمن أهم المؤسسات التي تنهض بمهمة صياغة السياسات وتأطير الاستراتيجية الوطنية للمعلومات والاتصالات في البلاد. وقد التحق بهذه الطبقة مجموعة من المجالس والهيئات العليا التي ارتبطت بقمة الهرم الذي يدير دفة البلاد، واوكلت لها مهمة اقتراح استراتيجية تشكيل الفضاء السيبراني والاتصالات الإيراني، وتحديد المحددات الوطنية لاستخداماته، وبيان مواطن التهديدات المحتملة لخطاطة الثورة الإسلامية، أو استغلال الفجوات السيبرانية لتهديد الأمن القومي للبلاد.

وقد أولت هذه الهيئات والمجال العليا ا هتماماً خاصاً فجعلت إدارتها ممثلة برئيس البلاد، وعضوية قيادات عليا من المؤسسات التشريعية، والعقدية، والحرس الثوري الإيراني، ووزراء من الحكومة، وأعضاء من من التيارات المتشددة بالبلاد، لضمان إحكام السيطرة على تخوم الفضاء، ومجاله الاتصالي.

الطبقة الوسيطة: الوزارة المعنيّة ومؤسسات وشركات تنفيذية:

وتضم وزارة تقنية المعلومات والاتصالات مع مجموعة من المؤسسات والشركات التي تنهض بمهام تنفيذ السياسات التي تعد في أروقة مؤسسات الطبقة العليا، وترجمتها الى إجراءات تتوافق مع السياقات التقنية التي تعتمد في قطاع المعلومات والاتصالات.

وتتميز هذه الوحدات التنظيمية بكونها ذات صبغة تقنية وتنفيذية صرفه، ولا تمتلك سقفاً للصلاحيات يسمح لها بنقض، او تخصيص مجال القرارات التي تتخذ في أروقة الطبقة العليا، وتناط بها على الدوام عملية تنفيذها مهما كان حجم الجهد التقني، أو التخصيصات المالية المطلوبة لترجمة الاستراتيجية الى مشاريع تستوطن بيئة المعلومات والاتصالات الإيرانية.

الطبقة الدنيا: مؤسسات حماية الفضاء السيبراني وكف الجريمة عن حياضه:

وتتألف من مجموعة المؤسسات والهياكل التنظيمية التي تمارس إجراءات لكف عمليات تجاوز الحدود التشريعية والتعليمات التي شرعت لحماية امن المعلومات ومكافحة الجرائم السيبرانية. وتستوطن في هذه الطبقة وحدة شرطة الفضاء السيبراني (*FATA*) *Cyber Police Unit*، والمجلس الأعلى للأمن الوطني *The High Council of National Security* (*HCNS*).

2 . 1 . المجالس والهيئات العليا:

لقد تكاثر عدد المجالس العليا والهيئات التي كلفت بمهام ذات صلة بإدارة وتنظيم الفضاء السيبراني بإيران، خلال العقد الأول من الألفية الجديدة، وحصل تداخل كبير في المهام التي أنيطت بها، مع تعدد الجهات التي ترتبط بها أو تتلقى منها تعليمات مباشرة، واوامر صارمة لترويج سياساتها الأمنية، أو العقدية، الأمر الذي أورث هذه المؤسسات، والبيئة الحاضنة لالفضاء السيبراني والاتصالات، والتطبيقات والخدمات الملتحقة بها، المزيد من آثار التجاذبات الحادة، وتناقض الآراء الحاكمة لعملية إدارة المهام، وصياغة السياسات الوطنية.

واستمرت عملية صناعة القرارات الحكومية بخصوص قطاع المعلومات والاتصالات، تتأرجح بين المجلس الأعلى للمعلوماتية ووزارة تقنية المعلومات والاتصالات، من جهة، والمجلس الأعلى لتقنية المعلومات والاتصالات، والمجلس الأعلى لنشر المعلومات، من جهة أخرى. ويلاحظ أن جهات الطرف الأول كانت ملتحقة بالمؤسسة المسؤولة عن عمليتي الإدارة والتخطيط في البلاد، بينما انتمت جهات الطرف الثاني وجاهرت بولائها المطلق لخطاطة المجلس الأعلى لثقافة الثورة الإسلامية (Davarinejad&Saffari,2010).

2 . 1 . 1 . المجلس الأعلى للمعلوماتية:

يعد المجلس الأعلى للمعلوماتية *High Council of Informatics* (*HCI*) أول هيكل تنظيمي فوّضه المجلس الأعلى للثورة الإسلامية في عام 1979، للنهوض بمهمة متابعة، واتخاذ القرارات ذات الصلة باستخدام وتوطين الحواسب بإيران (*Davarinejad&Saffari,2010*). وقد اقتصرت أنشطة هذا المجال، في السنوات الأولى التي تلت إنشائه، بحلحلة المشاكل، وإدارة الأزمات مع شركات الحواسب الغربية، التي أرادت مغادرة البلاد عند تصاعد أوار أزمتها مع الولايات المتحدة، واندلاع حربها مع العراق.

وقد تراجع الدور الذي مارسه هذا المجلس، مع بدايات عام 2001، عندما أبصر النور هيكل تنظيمي جديد أطلق عليه " المجلس الأعلى لنشر المعلومات *High Council of Information Dissemination* (*HCID*) والذي عزّز وجوده على ساحة المؤسسة السيبرانية الإيرانية بإطلاق مبادرة "تنمية تطبيقات تقنية المعلومات" والتي أطلق عليها باللغة الفارسية اصطلاح *TAKFA*.

ولم تمر سوى سنتين حتى شهدت إيران ولادة مؤسسة معلوماتية جديدة، أطلق عليها المجلس الأعلى لتقنية المعلومات *Supreme Council of Information Technology* (*SCIT*) بعد أن صدر قانون بشأن تأسيسه في عام 2003.

ارتبط هذا الهيكل التنظيمي بمكتب رئيس الجمهورية الذي تبوأ منصب رئيس الهيئة، وقد أنيط بالهيئة جملة من المهام والمسؤوليات ـ التخطيطية، ذات الصلة بتطوير قطاع المعلومات والاتصالات في إيران، والتي تضمنت (*Jahangard,2004*):

- ✓ إعداد الإطار العام والتفصيلي لسياسات قطاع تقنية المعلومات والاتصالات بالبلاد مع توفير المشورة والدعم التقني.
- ✓ التخطيط لمستقبل تقنيات المعلومات والاتصالات بالبلاد.
- ✓ وضع الخطط الوطنية فرق العمل التي تعمل تحت مظلة المركز.
- ✓ انتخاب التطبيقات والخدمات التي تلبي حاجات المستخدم الإيراني في نطاق قطاع المعلومات والاتصالات.

كذلك، وقد أشرف المجلس الأعلى لتقنيات المعلومات والاتصالات *SCICT* على إعداد وهيكلة مكونات مشروع *TAKFA* خلال السنوات 1999-2002 لكي تتوافق أهداف المشروع مع الإطار العام للسياسات التي تختطها للبلاد (*Khanmesan,2010*).

وعلى صعيد آخر، أوكلت للمجلس مهمة التواصل والتنسيق مع القطاعين الحكومي والقطاع الخاص، لاقتراح صيغ القوانين والتعليمات، وإعداد خطط مشاريع القطاع بالتنسيق مع الوزارات المختلفة، من جهة، وتنظيم السياسات وتلبية احتياجات القطاع الخاص ومنظمات المجتمع المدني التي تعمل ضمن نطاق قطاع المعلومات والاتصالات.

لم يقتصر مضمون القانون على إنشاء المجلس الجديد، وإنما ذهب الى توسيع دائرة مهام وزارة الاتصالات وإدارة الترددات الراديوية، بعد أن أناط بها مهمة إعداد خطط واستراتيجيات تقنية المعلومات ـ الوطنية، وتحديد معالم سياسات نشر تقنية المعلومات وادواتها ضمن قطاعات الأنشطة: الاجتماعية، والاقتصادية، والثقافية في عموم إيران. كما اوكل لها مهمة تشكيل هيكلة تنظيمية، تعمل على تنفيذ السياسات المصادق عليها من قبل المجلس الأعلى، على طريق إعادة هيكلة قطاع الاتصالات، وتحديد ومراقبة طيف الترددات الراديوية الوطنية.

2 . 1 . 2 . المركز الوطني للفضاء السيبراني:

أنشئ المركز الوطني لالفضاء السيبراني *National Center of Cyberspace NCC* بأمر مباشر من قبل المرشد الأعلى للثورة الإسلامية، وأوكلت للمجلس الأعلى لالفضاء السيبراني مهمة تحديد أهدافه بما يتوافق مع رؤية القائد الأعلى. وقد صودق على قانون المركز في الربع الأخير من عام 2013، وأوكلت للمركز حزمة كبيرة من المهام ذات الصلة بالحضور الإيراني في فضاء الانترنيت العولمي، والتي يمكن إجمالها بما يأتي (*SMO,2015d*):

- ✓ ترسيخ استقلالية إيران في مجال الخدمات السيبرانية وبناها التحتية، من خلال التركيز على تطوير مضيفات مواقع الويب الإيرانية دون الحاجة الى دعم دول أخرى.
- ✓ دعم وتشجيع إنتاج المحتوى السيبراني ـ المحلي لتلبية احتياجات المستخدمين المحليين، وتركيز الاهتمام بالمحتويين العقدي والأيديولوجي، مع الاهتمام بالانفتاح على الآخر.
- ✓ ترسيخ الوعي لدى المواطن بمسائل الأمن السيبراني، وتطبيق ممارساته السليمة للحفاظ على حواسبهم، ومواردهم السيبرانية من عمليات التلصص والقرصنة السيبرانية.
- ✓ تنظيم عمليات تبادل المعلومات مع الشبكات الدولية، وتوظيف شبكة الانترنيت الوطنية *SHOMA* للفصل بين المرور السيبراني الوطني والعولمي، لحماية الموارد الوطنية من عمليات التسلل والقرصنة.
- ✓ توفير متطلبات خوض غمار الحرب الناعمة التي يستهدف بها الفضاء السيبراني الإيراني وبنيته التحتية من قبل أعداء الثورة الإسلامية.
- ✓ حماية الفضاء السيبراني الوطني من التهديدات والهجمات السيبرانية التي تمارس من تخوم فضاء الانترنيت العولمي.
- ✓ مد جسور التعاون مع شعوب وحكومات تشترك مع إيران في تعرضها للمخاطر السيبرانية الناتجة عن هيمنة الولايات المتحدة على الفضاء السيبراني العولمي، والدعوة الى حماية حقوق المستخدم إزاء الاحتكار الذي تمارسه هذه الدول.

أما مهامه على صعيد إدارة وتنظيم، وحماية الفضاء السيبراني الإيراني الممتد على عموم الرقعة الجغرافية للبلاد، فقد حددت من خلال احدى وعشرين فقرة، لعل أهمها (*SMO,2015d*):

- التخطيط بعيد الأمد لاستنبات وتطوير آلة وادوات القدرات السيبرانية الناعمة في إيران، مع بث الخطاب العقدي والأيديولوجي للثورة الإسلامية في فضاء الانترنيت العولمي.
- مراجعة وتقييم الخطط الوطنية ذات الصلة بتوسيع وتطوير تخوم الفضاء السيبراني الوطني، مثل مشروع شبكة الانترنيت الوطنية *SHOMA*، ومشروع تلفاز الانترنيت *IPTV*، وخدمات التلفاز الآنية *On-Demand TV Services*.
- تشجيع القطاع الخاص على المساهمة الفاعلة في إرساء بنيان الفضاء السيبراني الإيراني، وإثراء المحتوى وتوسيع نطاق الخدمات السيبرانية المطروحة للمستخدم الإيراني.
- تشجيع مراكز البحوث الوطنية، والمؤسسات الأكاديمية، وشركات القطاع الخاص على إنتاج برمجيات المراقبة، وتقطير المحتوى السيبراني للمواقع التي تطرح محتوى يخالف خطاطة الثورة الإسلامية وثقافتها الملتزمة.

أما الهيكل التنظيمي للمركز فقد ضم في تركيبته المؤسساتية ثلاث هيئات عليا تمارس أنشطتها المختلفة لدعم المجلس الأعلى لالفضاء السيبراني وتوفير مناخ مناسب لصناعة القرارات على أرضية صلبة. وهذه الهيئات هي:

1. الهيئة العليا لتنظيم سياسة الفضاء السيبراني The Supreme Committee of Cyberspace Regulation (SCCPR).
2. الهيئة العليا لتحسين وإنتاج محتوى الفضاء السيبراني The Supreme Committee for the Improvement and Production of Cyberspace Content (SCIPCC).
3. الهيئة العليا لأمن الفضاء السيبراني The Supreme Committee of Cyberspace Security (SCCS).

2 . 1 . 3 . المجلس الأعلى للفضاء السيبراني *SCC*:

أصدر القائد الأعلى، آية الله علي خامنئي، في 7 مارس من عام 2012، أمراً بتشكيل المجلس الأعلى لالفضاء السيبراني *The Supreme Council of Cyberspace SCC* للنهوض بمهام إعداد وتنظيم، والاشراف على سياسة الفضاء السيبراني في إيران، وأن يكون البديل النهائي للمجالس العليا التي سبقته (*SMO,2014,a*).

لقد أراد القائد الأعلى للثورة الإسلامية في إيران، لهذا المجلس أن يعتلي قمة هرم المؤسسات التنظيمية لإدارة المعلومات والا تصالات في البلاد، وتخويله طيفاً واسعاً من الصلاحيات لضمان إدامة متطلبات بيئة آمنة لالفضاء السيبراني وفق المعايير العقدية لثقافة الثورة، مع إدامة مستوى مقبول من الأمن السيبراني الوطني لدرء مخاطر الحرب الناعمة مع الشيطان الأكبر، وبقية النظم الغربية التي تناصب الثورة العداء، وتحاول بشتى الطرق إحداث فجوات في المناخ الثقافي الذي جاءت به الثورة الإسلامية.

أولاً. أهداف المجلس وغاياته:

أرادت القيادات العليا في إيران، وبجميع مستوياتها، أن تحكم قبضتها على الفضاء المفتوح للأنترنيت وتضمن حصانة مؤسسات البلاد، وسكانه قبالة التحديات العقدية، والثورية، والاجتماعية التي أضحى الفضاء مرتعاً مناسباً لاحتضانها وتنميتها، من خلال مؤسسة تنظيمية عليا، وفرت لها نطاقاً واسعاً من الصلاحيات، وعززّت نشاطها بدعم مالي ولوجستي غير مسبوق، وألحقت بمجلسها نخبة من قيادات الثورة ومؤسساتها الحكومية، وعلماء البلاد، وبمختلف الانتماءات لكي يستطيع المجلس صياغة سياسات على الأمد القريب، واستراتيجية بعيد المدى تنظّم مكونات النظام وخدماته وتوجه دفة أنشطته بحيث تتوافق مع سياستها وخطاطتها العقدية، وتحمي البلاد من المخاطر الناعمة التي أضيفت الى المخاطر التقليدية التي تقضّ مضاجع المؤسستين العسكرية والأمنية بالبلاد.

ولقد وضع المجلس في مقام يقع خارج نطاق التأثيرات المباشرة التي يمكن أن يمارسها المجلس الإيراني، لغرض التخفيف من وطأة التأثيرات المحتملة، والتي يمكن أن تمارس عليه، ولإبعاده قدر المستطاع عن التجاذبات وتنازع السلطات، التي يمكن أن ينشب عنها حصول فجوة، قد تؤدي الى تسلل المخاطر السيبرانية للبلاد.

بصورة عامة أفصحت القيادة الإيرانية عن هدفين أساسيين لإنشاء هذا المجلس (*SMO,2014,a*):

الهدف الأول: استثمار الجوانب الإيجابية من فضاء الانترنيت في توسيع دائرة انتشار خطاب الثورة الإسلامية ودعم الأنشطة التنموية بالبلاد، وبناء القدرات السيبرانية للموارد البشرية الوطنية.

الهدف الثاني: حماية البلاد والشعب الإيراني من التهديدات والمخاطر التي تستبطن في الجزء المظلم من فضاء الانترنيت.

ومما لا ريب فيه، وجود أهداف أخرى لم تفصح عنها القيادة الإيرانية حول أهداف المركز الأعلى لالفضاء السيبراني وغاياته، بيد أن من الأهداف الرئيسة هو الرغبة في اقصاء الهيكلة التنظيمية عن ساحة النزاعات والتجاذبات عن ساحة مؤثرة، مع تصاعد التهديدات المحتملة بعد الهجمات التي نجحت في بلوغ منظومات تشغيل أجهزة الطرد المركزي في المشروع النووي الإيراني، وتأجيج النزاع بين المعارضة والحكومة كلما سنحت الفرصة لذلك، مع تعاظم إقبال المواطنين الإيرانيين على الفضاء الجديد بحيث لم يعد من الممكن حظرها، مع عدم نجاعة عمليات الحظر والحجب نتيجة لتكاثر أدوات تجاوز الجدران السيبرانية، والمطروحة بالمجان على مواقع الانترنيت، والتي تدعم وفرتها الولايات المتحدة وإسرائيل لإدامة وجود ثغرات وفجوات تدعم محاولات المواطن الإيراني على تسريب خطابه المعارض، وبلوغ المواقع المحظورة بعيداً عن أنظار منظومة المراقبة الايرانية.

ثانياً. الهيكل التنظيمي للمجلس:

حدد قرار القائد الأعلى للثورة الإسلامية عديد أعضاء المجلس الأعلى لالفضاء السيبراني، بعشرين عضواً، تساهم الكابينة الحكومية والمؤسسات الحكومية بثلاثة عشر عضواً منهم، بينما يقوم القائد الأعلى بتسمية سبعة أفراد لإكمال نصاب الهيكل التنظيمي لأعضاء المجلس الأعلى (*SMO,2014,a*).

بيد أن عدد الأعضاء قد تجاوز القرار الابتدائي للهيكل التنظيمي بعد أن زيد في عدد الأعضاء الذي قام بتسميتهم القائد الأعلى من سبعة أعضاء الى تسعة أعضاء (فأصبح العدد الكلي لأعضاء المجلس الأعلى اثنان وعشرون عضواً بدلاً من عشرين) دون أن يفصح مكتب القائد الأعلى عن سبب هذه الزيادة (*SMO,2014,a*).

ومع حلول عام 2015 أصبح عدد أعضاء المجلس الأعلى ستة وعشرين عضواً، بعد أن ازدادت حصة الكابينة الحكومي ومؤسسات الحكومة الى سبعة عشر عضواً، مع بقاء عدد الأفراد الذين يسميهم القائد الأعلى (بصورة مباشرة) وانحصارهم بتسعة أعضاء فقط.

وقد تألف فريق القطاع الحكومي من تسعة أعضاء التحقوا من الكابينة الحكومية لحسن روحاني[66]، أما البقية فقد رشحهم القائد الأعلى من القطاع الحكومي، ومن مؤسسات حكومية مختلفة[67] (*SMO,2015d*).

ويمكن قراءة الأرضية التي تنطلق منها قرارات هذه الهيكلة التنظيمية من خلال مراجعة خارطة انتماءات أعضاء المجلس الأعلى خلال السنوات 2013-2015 ـ أنظر الجدول (3 - 2).

---

[66] . شملت هذه المجموعة الرئيس حسن روحاني بصفته رئيس المجلس، ووزير تقنية المعلومات والاتصالات، ووزير الثقافة والإرشاد الإسلامي، وآخرين من الكابينة الحكومية.

[67] . من أعضاء هذه المجموعة: رئيس السلطة التشريعية بإيران، والقائد الأعلى للحرس الثوري الإيراني، ورئيس الاعلام وإذاعة الثورة الإسلامية بإيران.

الجدول (3 - 2) ـ خارطة انتماءات أعضاء المجلس الأعلى للفضاء السيبراني الإيراني خلال السنوات 2013-2015[68].

السنة	نسب فئات أعضاء المجلس الأعلى للفضاء السيبراني			
	المتشددون	المحافظون	المعتدلون	المستقلين
2013	% 27	% 32	% 23	% 18
2015	% 27	% 27	% 35	% 11

ومن الواضح أن فئة المتشددين والمحافظين تشكّل الأكثرية من أعضاء المجلس الأعلى (54-59 %) الأمر الذي يرجّح كفة القرارات التي يريدها القائد الأعلى، والمؤسسات الأمنية والعسكرية قبالة أي مقترح قد يتقدم به أحد الأعضاء المعتدلين، مع وجود نسبة من الأفراد المستقلين التي تزيد نسبة حضورها على 10 %، الأمر الذي يضمن إحباط أي محاولة إصلاحية، والهيمنة الدائمة للخطاطة المتشددة في التعامل مع فضاء الانترنيت في إيران، ويبدو هذا الأمر واضحاً في الولاء المستمر ومحاولة استرضاء الأعضاء للقائد الأعلى (في قراراتهم) على حساب سياسة روحاني والملتحقين بدائرته من مسؤولين في الكابينة الحكومية.

لذا فمن غير المتوقع حصول تغييرات حاسمة في سياسة واستراتيجية المعلومات والاتصالات بالأفق المنظور، في ظل هذه التركيبة من أعضاء المجلس، والتي لن توفر فرصة لتمرير أي إصلاح ينحو نحو الاعتدال في التعامل مع ملف الفضاء السيبراني الايراني.

ثالثاً. اسهامات المجلس الأعلى للفضاء السيبراني:

إن الصلاحيات الواسعة التي منحت للمجلس الأعلى للفضاء السيبراني، مع تسنّم رئيس الجمهورية الإيرانية منصب رئاسة المجلس، ووفرة التخصيصات المالية للمجلس[69] قد منحت للمجلس فضاءً واسعاً في اتخاذ قرارات حاسمة، وعلى أرضية راسخة ومتينة.

وقد وضع المجلس خططاً بعيدة الأمد، منذ نهاية عام 2012، لإدارة وتنظيم الفضاء السيبراني الإيراني وفق الخطاطة التي أرادها القائد الأعلى للثورة الإيرانية بإيران، تضمنت فقراتها:

- ✓ تحسين الخصائص والقدرات الأمنية والدفاعية للفضاء السيبراني.
- ✓ تطوير عملية إنتاج المحتوى السيبراني، والارتقاء بمادة ومضامين المحتوى.
- ✓ تطوير الخدمات السيبرانية ـ المطروحة في الفضاء السيبراني الإيراني.
- ✓ تحسين وتطوير البنية التحتية للفضاء السيبراني والاتصالات.
- ✓ تطوير ودعم مشاريع البحث والتطوير في قطاع المعلومات والاتصالات، سواء على صعيد الاستراتيجية وثقافة الاستخدام.
- ✓ إعداد خطاطة وطنية، واضحة المعالم، لتنظيم الحضور السيبراني في الفضاء السيبراني.

ولم تغب عن اهتمامات المجلس الأعلى للفضاء السيبراني، المسائل التفصيلية، والتي ترده ضمن التوجيهات المستمرة من مكتب القائد الأعلى، أو الجهات التي تمتلك ناصية الملفات الأمنية والعقدية بالبلاد. فقد استمرت بإصدار تعليمات

[68] . قام المؤلف بإعداد هذا الجدول من البيانات المذكورة في المصدرين:(*SMO,2014,a*)| (*SMO,2015d*).

[69] . حيث بلغت تخصيصاته لعام 2014 حوالي 40 مليون دولار، بينما زيدت تخصيصاته لعام 2015 الى حوالي 50 مليون دولار (*SMO,2015d*).

حول حظر بعض منصات التواصل الاجتماعي، وقامت بمتابعة عمليات الحظر والمراقبة، كما حددت صلاحيات المؤسسات المختلفة بالتعامل مع ملفات الفضاء السيبراني، والمراجعة الدائمة لقرارات وزارات الدولة ذات الصلة بالفضاء السيبراني، إصدار تراخيص شبكات الهواتف المحمولة *3G, 4G*، والاستمرار بتطوير شبكة الانترنيت الوطنية *SHOMA*، ومسائل أخرى ذات صلة بواقع الفضاء السيبراني في إيران (*SMO,2015d*).

2. 1. 4. هيئة تقدير حالات المحتوى الجنائي *CDICC*:

أنشئت هيئة تقدير حالات المحتوى الجنائي *The Commission to Determine The Instances of Criminal Content* (*CDICC*) ، في شهر مايو من عام 2009، بناء على ما جاء في الفقرة 22 من قانون جرائم الفضاء السيبراني التي أعطت للسلطة القانونية في إيران صلاحية تشكيل هذه الهيئة لتعمل تحت مظلة مكتب المدعي العام الإيراني. وقد أفصحت الحكومة عن طبيعة المهام التي أوكلت لهذه الهيئة وهي مهمة مراقبة قنوات ومحتوى الفضاء السيبراني، مع الحرص على ترشيح مادة المحتوى الجنائي من الفيض السيبراني لمواقع الانترنيت[70].

تضم الهيئة ثلاثة عشر عضواً رفيعاً هم: المدعي العام في إيران، ووزير المخابرات، ووزير الثقافة والإرشاد الإسلامي، ووزير العدل، ووزير تقنية المعلومات والاتصالات، ووزير العلوم والبحث والتقنية، ووزير التعليم، والقائد العام للشرطة، ورئيس الشؤون الثقافة والاعلام في منظمة التنمية الإسلامية *Islamic Development Organization* (*IDO*)، ورئيس هيئة الإذاعة في الجمهورية الإسلامية بإيران، وخبير بمجال تقنية المعلومات والاتصالات تسميه لجنة الصناعة والتعدين البرلمانية، قانوني ترشحه وزارة العدل ويصادق البرلمان على تسميته، وممثل عن المجلس الأعلى لالفضاء السيبراني (*SMO,2014,b*).

احتلت هذه الهيئة قمة هرم إدارة الفضاء السيبراني في إيران حتى عام 2012 حيث كانت ولادة المجلس الأعلى لالفضاء السيبراني الذي أصبح مسؤولاً عن صناعة سياسات السيبرانية واستراتيجيتها، إلا أن هذه الهيئة لا زالت تتمتع بسلطة المعالجة الآنية التي تتعلق بمسائل الحظر، وترشيح محتوى صفحات الويب، وتستمر بتنازع السلطة مع المجلس والإدارات الحكومية العليا بالبلاد بحسب الضغوط التي تمارسها مؤسسة الحرس الثوري، والتيار المتشدد في المجلس الإيراني.

2 . 2 . الجهات التنفيذية:

حوت كابينة الحكومة الإيرانية مجموعة من الهيئات التنفيذية التي تعنى بملف الاتصالات والمعلومات في إيران. وتتدرج هذه الهيئات من هياكل تنظيمية لوزارات، ومؤسسات تقنية، ومراكز بحوث، وشركات قابضة تتقاسم فيما بينها المهام التنفيذية لأنشطة الاتصالات والمعلومات في عموم إيران.

2 . 2 . 1 . وزارة تقنية المعلومات والاتصالات:

لإيران تاريخ عريق على صعيد الخدمات الاتصالية، فقد امتلكت أول مكتب للخدمات البريدية قبل عام 1876 والذي تحوّل الى وزارة لإدارة الخدمات البريدية *M.P* في عام 1877. ومع بدايات القرن العشرين التحقت خدمة التلغراف مع الخدمات البريدية فأضحت الوزارة تحمل اسماً جديداً هو وزارة البريد والتلغراف *Ministry of Post & Telegraph*. وتقدمت الوزارة الى البرلمان الإيراني بطلب لشراء حصة الخدمات الهاتفية عند نهاية عام 1929

[70] . تحاط الكثير من المهام التي تمارسها هذه الهيئة، وغاياتها الحقيقية، بسحابة اصطنعتها الإدارة الإيرانية نظراً لأهمية الدور الذي تمارسه على صعيد حماية الفضاء السيبراني الإيراني من التهديدات التي قد تمارس ضد النظام الإيراني وخطاطته العقدية والعسكرية والفكرية. لذا لا زال الغموض يلف الكثير من أنشطة الهيئة شأن بقية المؤسسات العسكرية والأمنية الإيرانية.

ليصبح اسمها وزارة البريد والتلغراف والهاتف *Ministry of Post, Telegraph & Telephone*، والذي احتفظت به لغاية عام 2003 (*Wikipedia,2015*).

وفي عام 2003 عمد المجلس الإيراني الى إصدار تشريع تحولت بموجبه هذه الوزارة العريقة الى وزارة تقنية المعلومات والاتصالات *Ministry of I.C.T* والتي بدأت ببسط سلطانها على ساحة فضمت إليها، مع حلول عام 2005، شركة بيانات الاتصالات *Data Communication Company D.C.C* بعد أن تحوّل اسمها الى شركة اتصالات إيران *I.C.T*، مع تأسيس شركتين التحقتا معها هما شركة *T.I.C* وشركة *I.R.I*.

وقد أضيفت للوزارة الجديد حزمة من المهام الجديدة، توافقت مع طبيعة التغييرات الحاصلة في تسميتها، فأدرجت في قائمة مهامها تلك التي تناظر خدمات المعلومات وتنظيم فضاء الانترنيت، فتوسعت الدائرة وباتت الوزارة مسؤولة عن المحاور الثلاثة للاتصال والمعلومات: البريد، والخدمات الهاتفية الأرضية والمحمولة، وخدمات المعلومات التي تشكّل شبكة الانترنيت العصب الحيوي لمادة نسيجها الشبكاتي.

وتضم وزارة تقنية المعلومات والاتصالات مجموعة من المؤسسات التي تدعم همها في قطاع تقنية المعلومات والاتصالات بالبلاد، نذكر منها:

- ✓ السلطة التنظيمية لاتصالات إيران *Communication Regulatory Authority Commission (CRA)* والتي تقوم بعملية الاشراف على ممارسات الجهات الاتصالية، وتحديد إطار تسعير السلع والخدمات، وتنظيم قواعد التعريفة بما يضمن حماية المستخدم، وتحديد مستويات جودة الخدمة السيبرانية والاتصالية، ومعايير تقييمها.
- ✓ المجلس الأعلى لتقنية المعلومات *High Council of IT (HCIT)* والذي تعكف كوادره الخبيرة على صياغة وتقنين أهداف استراتيجية المعلومات في البلاد، إعداد الإطار العام لسياسات واستراتيجيات لتنمية استخدام أدوات المعلومات والاتصالات في البلاد بمجالات متعددة، صياغة القواعد والتنظيمات الحاكمة لأدوات المعلومات والاتصالات، وتقنين مجالات خطط التعاون الدولي بهذا المضمار.
- ✓ مركز بحوث اتصالات إيران. *Iran Telecommunication Research Center (ITRC)* والذي يعد أهم مركز بحثي بالبلاد يمارس أنشطة البحث والتطوير في قطاع المعلومات والاتصالات منذ أربعة عقود، مع توفير المشورة العلمية والتقنية للوزارة.

ويضاف الى ذلك الحضور المميز لشركة اتصالات إيران. *Telecommunication Company of Iran (TCI)* وهي شركة تلتحق بالقطاع الحكومي أنشئت عام 1971 لإدارة جميع تفاصيل ملف الاتصالات في إيران. وتحولت بعد حين الى شركة قابضة انضوت تحت مظلتها مجموعة من الشركات التي تركز اهتمامها بتوسيع شبكات الاتصالات وتوفير الخدمات للمواطن الإيراني، والمؤسسات الحكومية. ومن شركاتها الثانوية: شركة البنية التحتية للاتصالات *TIC*، وشركة إيران للاتصالات المحمولة *MCI*، وشركة اتصالات البيانات *DCI*، بالإضافة الى أكثر من شركة اتصالات تتوزع بين المحافظات الإيرانية المختلفة.

2 . 2 . 2 . وكالة تقنية المعلومات والاتصالات الوطنية:

تنتمي وكالة تقنيات المعلومات والاتصالات الوطنية *National ICT Agency (NICTA)*، الى المؤسسات الحكومية المسؤولة عن تطوير سياسات واستراتيجيات قطاع المعلومات والاتصالات. وقد أوكلت إليها كذلك كافة المهام ذات الصلة بمبادرات تقنية المعلومات والاتصالات مع تقديم الخطط التنفيذية الخاصة بمشروع *TAKFA* الذي يشمل

السياسة الإيرانية ـ الوطنية لتنمية وتطوير البيئة الحاضنة لتوطين تقنية المعلومات والاتصالات بالبلاد، مع توسيع رقعة استخدام تطبيقاتها المختلفة (*Khanmesan,2010*).

2 . 3 . مؤسسات أمن المعلومات ومكافحة جرائم المعلومات:

تمارس هذه المؤسسات والهيئات مهمة تنفيذ التشريعات الخاصة بحدود استخدام الفضاء السيبراني والتطبيقات المطروحة في فضائه السيبراني، ومكافحة جرائم المعلومات والتجاوز على خصوصيات المستخدمين، سواء كان عملهم داخل حدود المؤسسات الحكومية، أو شركات قطاع التجارة والأعمال، والسعي الى كف عمليات اختراق نزم معلومات المصارف الالكترونية بالبلاد.

وبالوقت ذاته تمارس هذه المؤسسات دور الرقيب على أنماط استخدام التطبيقات المتوفرة على الانترنيت، وتراقب عن كثب عمليات تجاوز جدران الحظر السيبراني، أو طرح محتوى رقمي على مواقع الانترنيت، أو شبكات التواصل الاجتماعي قد يتعارض مع اهداف الثورة الإسلامية وخطاطتها العقدية، أو يشكل تهديداً امنياً للبلاد.

ومن هذه المؤسسات:

- ✓ المجلس العالي لأمن تبادل المعلومات في الفضاء السيبراني *High Council of Cyberspace Information Exchange Security (AFTA)* الذي يرتبط بمكتب رئيس الجمهورية ويتحمل مسؤولية الشؤون الأمنية لتبادل المعلومات بين المؤسسات الحكومية بإيران (*Davarinejad&Saffari,2010*).
- ✓ شرطة الفضاء السيبراني *Iranian Cyber Police (FATA)* وهي مؤسسة امنية خطط لتشكيلها منذ عام 2009، بعيد الأحداث التي عصفت بإيران عند الحملة الانتخابية واستخدام شبكات التواصل الاجتماعي من قبل الناشطين المعارضين للحكومة الإيرانية. وقد أبصرت النور في 23 يناير عام 2011 وأعلن عنها بوصفها مؤسسة شرطية لمكافحة جرائم الانترنيت. استقرت الوحدة الأولى بالعاصمة طهران، ثم انتشرت فروعها في بقية المحافظات الإيرانية، وتمارس هذه المؤسسة دوراً سياسياً إضافة الى محاربتها للجرائم السيبرانية، وذلك من خلال ملاحقة الحضور السيبراني للناشطين السياسيين، أو استخدام شبكات التواصل الاجتماعي، أو المواقع التي تحظرها الحكومة في نشر خطاب معارض للسلطة أو خطاطة الثورة الإسلامية.

3 . السياسة والرؤية السيبرانية الإيرانية:

يمكن تمثيل رؤية وسياسة مؤسسة الدولة الإسلامية في إيران (لإدارة وتنظيم وتطوير بيئة المعلومات والاتصالات) بمعمارية هرمية تتألف قاعدتها من ممارسات سياسة المعلومات التي تشمل: صناعة القرارات، ومراقبة وتنظيم وإدارة العمليات التي تسري في قطاع المعلومات والاتصالات، من جهة، والكيانات والهيئات التي تنهض بمهمة حوكمة الفضاء السيبراني والاتصالات، من جهة أخرى (*ITU,2013*).

أما الطبقة الوسيطة فتؤلف العناصر البنيوية لاستراتيجية الدولة في التعامل مع قطاعات:

- ✓ الحكومة الالكترونية.
- ✓ قطاع التجارة والمصارف الالكترونية.
- ✓ الثقافة الإسلامية الإيرانية في الفضاء السيبراني.
- ✓ الصحة الالكترونية ومقومات الرفاه السيبراني.
- ✓ البنية التحتية للمعلومات والاتصالات.
- ✓ أمن المعلومات.

✓ قوانين وتنظيمات بيئة المعلومات والاتصالات.

أما الاستراتيجية الوطنية لقطاع المعلومات والاتصالات فتستوطن قمة هذا الهرم حيث تسود رؤية الدولة وسياستها في كيفية التعامل مع عناصر منظومة هذا القطاع الحيوي.

وتسسهم أكثر من جهة عليا في تشكيل عناصر هذه الرؤيا، فتبدأ إرهاصاتها لدى القائد الأعلى للثورة السيد علي خامنئي حيث يصدر توجيهاته التي تؤطر أهم معالم الرؤية السياسية والعقدية لاستراتيجية المعلومات لكي يتلقفها المجلس الأعلى لالفضاء السيبراني ويحول هذه الأطر العامة الى رؤية وسياسة معلوماتية أكثر تفصيلاً تتوافق مع متطلبات بقية طبقات المعمارية الهرمية وبعد أن يضع ممثلي الجهات المتنفذة في صناعة القرارات بالبلاد بصماتهم على مداد الرؤية وتفاصيل السياسة السيبرانية بحيث تضمن كل جهة حضور هواجسها تجاه امتدادات رقعة الفضاء السيبراني في ساحة مسؤولياتها.

بصورة عامة يقوم المتشددين من أعضاء المجلس الأعلى، والحرس الثوري الإيراني بفرض المحددات الصارمة التي تضيّق الخناق على سياسة المعلومات والاتصالات بالبلاد، بينما يساهم رئيس الجمهورية وممثلي الوزارات التقنية في عملية التخفيف من وطأة التشديد الى الحدود التي يمكن أن يتوافق جميع أعضاء المجلس على التصويت عليها وإقرارها لكي تسافر نحو الطبقة التنفيذية حيث تمارس بقية المجالس والهيئات والوزارات التنفيذية بترجمة الاستراتيجية الى سياسات وإجراءات تلتزم بها بقية طبقات الهرم على صعيد تحديد معالم الفضاء السيبراني وتطبيقاته التي تتوافق مع جميع اطر الاستراتيجية الوطنية، بينما تعكف المؤسسات التشريعية والقانونية على إعداد التشريعات والقوانين والتعليمات التي تلزم المستخدمين، والقطاع الخاص، ومؤسسات الدولة على الالتزام بها لضمان توافق ممارسات المستخدمين مع المعايير التي حددتها استراتيجية الحكومة وسياساتها للحضور في الفضاء السيبراني واستخدام منصات تطبيقاته المتنوعة.

3 . 1 . ترجمة الرؤيا والسياسة السيبرانية الإيرانية على أرض الواقع:

تقوم الهيئات التنفيذية في قطاع المعلومات والاتصالات، في إيران، وعلى رأسها وزارة تقنية المعلومات والاتصالات بترجمة خطاطة الرؤية والسياسة التي كانت بداياتها في مكتب القائد الأعلى للثورة الإسلامية، وأعدت تفاصيلها في المجلس الأعلى لالفضاء السيبراني الى خطة تنفيذية تضمن نمو قطاع المعلومات والاتصالات بالبلاد مع التزامه بثقافة الثورة الإسلامية وأهدافها، وحفظ مكتسباتها من غوائل التهديدات الخارجية.

لقد اختطت وزارة تقنية المعلومات والاتصالات خطة في بدايات عام 2014 لضمان بلوغ البلاد الى مستوى رصين وفق معايير مجتمع المعلومات، وقامت بالتنسيق مع الوزارات والجهات الحكومية المعنية بتحقيق هذه الأهداف، بعد أن حددت معالم الأولويات التي تبنتها هذه الخطة الطموحة، والتي شملت المحاور التالية(*ITO,2014*):

1. **البنية التحتية الحاضنة في البلاد:**
   - 1.1. البنية التحتية للمعلومات والاتصالات.
   - 1.2. أمن المعلومات.
   - 1.3. الريع المتحقق وسبل الاستثمار في قطاع المعلومات والاتصالات.
   - 1.4. البحث والتطوير في قطاع المعلومات والاتصالات.
   - 1.5. الإطار القانوني الداعم لبيئة المعلومات والاتصالات.
   - 1.6. المحتوى السيبراني والحضور الثقافي بالفضاء السيبراني

2. **مجال التطبيقات السيبرانية.**

2.1. الحكومة الالكترونية.

2.2. الصحة الالكترونية.

2.3. التعليم الالكتروني.

2.4. التجارة الالكترونية.

2.5. المصارف الالكترونية.

2.6. القضاء الالكتروني.

غير أن هذه الخطة لم تحقق النجاح في جميع محاورها، نتيجة لوجود أكثر من ثغرة في نسيج البنية التحتية للمعلومات والاتصالات، من جهة، ووجود عقبات أنتجها الحصار المستمر على البلاد خلال حوالي عقد من الزمان، بالإضافة الى حضور ممانعة فرضها الواقع الاجتماعي، والسياسي على كثير من الأنشطة السيبرانية التي قد يؤدي غيابها الى عدم بلوغ الأهداف المرجوة لمثل هذه الخطط الطموحة (*ITO,2014*).

وإذا ابتدأنا مراجعتنا للمسألة الأكثر أهمية لدى النظام الإيراني، وهي مسألة ملف الأمن السيبراني ـ أنظر الجدول (3 - 3)، يبدو واضحاً أن ما تم تحقيقه على صعيد مراكز عمليات أمن المعلومات المحلية لم يتجاوز 20 % رغم أن المخطط كان 100 %، مع غياب أي نشاط على صعيد عمليات البنية التحتية، وبرمجيات وعتاد أمن المعلومات التي تصنّع محلياً، ونسب بوابات برمجيات الانترنيت الآمنة التي لم تتجاوز نسبة 6 % من النسبة المخططة، بينما قارب عدد مختبرات أمن المعلومات للكمية المخططة (28 مركزاً قبالة التخطيط لإنشاء 29 مركزاً).

الجدول (3 - 3) ـ الأهداف المرسومة لخطط أمن المعلومات ـ الخمسية في إيران (2009-2014).

الهدف	الغاية المرجوة عند نهاية الخطة	الحالة في عام 2014	نسب الانجاز
عدد المؤسسات الحكومية التي تعتمد نظام إدارة المعلومات ISMS وفق معايير أيزو 27001.	53 %	39 مؤسسة	...
نسبة مراكز عمليات أمن المعلومات المحلية.	100 %	20 %	20 %
نسب تنفيذ خطط CSIRT في المؤسسات الحكومية المركزية.	100 %	35 %	35 %
عدد مختبرات أمن المعلومات.	29	8	28
نسب تنفيذ عمليات البنية التحتية للمفتاح الأساسي PKI.	%100	...	0
نسب برمجيات وعتاد أمن المعلومات التي تصنّع محلياً.	70 %	...	0
نسب بوابات برمجيات الانترنيت المعيارية والآمنة	100 %	6 %	6 %

المصدر: *M.O.ICT,2015*

أما على صعيد الأهداف المرسومة لخطط تطوير البنية التحتية للمعلومات والاتصالات، فلا زالت البنية التحتية الإيرانية تعاني من نقص حاد على أرض الواقع، فلا زال العمل على سعة حزمة الانترنيت المحلية والدولية متراجعاً ولم تتجاوز نسبته 25-40 %، مع عدم كفاية أعداد مراكز المعلومات الفاعلة في البلاد. إلا أن وصول خدمة الانترنيت الى

المناطق الريفية قد حققت تقدماً لا بأس به فبلغت نسبة تحقيق الأهداف المرسومة أكثر من 60 % ـ أنظر الجدول (3 - 4).

الجدول (3 - 4) ـ الأهداف المرسومة لخطط تطوير البنية التحتية للمعلومات والاتصالات ـ الخمسية في إيران (2014-2009).

الهدف	الغاية المرجوة عند نهاية الخطة	الحالة في عام 2014	نسب الانجاز
سعة الحزمة الدولية للانترنيت (Gb/sec).	500	124	% 25
سعة الحزمة المحلية للانترنيت (Gb/sec).	2000	844	% 42
قدرة المشترك منسوبة لعدد السكان (مشترك).	843	260	% 31
عدد مراكز المعلومات Data Centers الفاعلة في البلاد.	40	18	%45
نسبة القرى التي تتألف من أكثر من 20 مسكن وترتبط بخدمة الهاتف.	100 %	78.8 %	79 %
نسبة القرى التي تتألف من أقل من 20 مسكن وترتبط بخدمة الهاتف العمومي المدفوع.	100 %	84.79 %	85 %
نسب القرى التي تمتلك أكثر من 70 منزلاً وتحتوي على مركز معلومات واتصالات،	100 %	15 %	15 %
نسب سكان الريف الذين تشملهم تغطية شبكات المحمول.	100 %	69.6 %	69.6 %
نسب المساكن الريفية التي ترتبط بخدمة الانترنيت.	60 %	17.5 %	%92
نسب المساكن المرتبطة بخدمة الانترنيت العريضة وترتبط بشبكة المعلومات الوطنية وبسعة لا تقل عن 512 Kb/sec.	60 %	38 %	63 %

المصدر: *M.O.ICT,2015*

ويبدو من بيانات الجدول (3 - 5) أن خدمة المصارف الالكترونية أوفر حظاً على صعيد تحقيق الأهداف المرسومة لها، فقد تجاوزت نسبة التسديد السيبراني النسبة المخططة بعد أن بلغت نسبتها 151 %، واستكملت المصارف الإيرانية نظمها السيبرانية المتكاملة، بينما لا زالت البنية التحتية للتوقيع السيبراني متراجعة بسبب تراجع ثقة الزبون الإيراني بها.

الجدول (3 - 5) ـ الأهداف المرسومة لخطط المصارف السيبرانية ـ الخمسية في إيران (2009-2014).

الهدف	الغاية المرجوة عند نهاية الخطة	الحالة في عام 2014	نسب الانجاز
نسبة حركة التسديد السيبراني منسوبة الى حركة النقد بالبلاد.	80 %	120.4 %	151 %
عدد المصارف التي تمتلك بنية تحتية للتوقيع السيبراني.	100 %	21 %	21 %
نسب المصارف التي تمتلك نظم رقمية متكاملة.	100 %	100 %	100 %

المصدر: *M.O.ICT,2015*

من جهة أخرى، تظهر بيانات الجدول (3 - 6) تراجع ما تم تحقيقه على أرض الواقع على صعيد التجارة الالكترونية، والتي تراجعت بجل محاورها.

الجدول (3 - 6) ـ الأهداف المرسومة لخطط تطوير أنشطة التجارة الالكترونية ـ الخمسية في إيران (2009-2014).

الهدف	الغاية المرجوة عند نهاية الخطة	الحالة في عام 2014	نسب الانجاز
نسبة أنشطة التجارة الالكترونية الأجنبية من الأنشطة الدولية.	100%	52.1 %	52.0 %
نسبة الشركات المرتبطة بشبكة المعلومات الوطنية.	20 %	...	...
نسبة الشركات المرتبطة بشبكة الانترنيت.	30 %	...	...

المصدر: *M.O.ICT,2015*

ورغم الاهتمام الكبير التي توليه الحكومة الإيرانية بتطوير منظومة حكومتها الالكترونية، إلا أنها لم تفلح بتحقيق أهدافها المرسومة إلا على صعيد ارتباطات مؤسساتها بشبكة المعلومات المحلية، وشبكة الانترنيت، بينما أخفقت في تحقيق بقية أهدافها، حيث تراجعت الخدمات الحكومية لقطاع التجارة والأعمال والقطاع الحكومي بشكل كبير، بينما لم تتجاوز نسبة الخدمات المطروحة للقطاع العام على 25 % ـ أنظر الجدول (3 - 7).

الجدول (3 - 7) ـ الأهداف المرسومة لخطط تطوير الحكومة الالكترونية ـ الخمسية في إيران (2009-2014).

الهدف	الغاية المرجوة عند نهاية الخطة	الحالة في عام 2014	نسب الانجاز
نسبة الخدمات الحكومية التي ستوفرها للمواطن G2C.	70 %	16.3 %	23 %
نسبة الخدمات الحكومية التي ستوفرها للتجارة والأعمال G2B	70 %	16.3 %	23 %
نسبة الخدمات الحكومية التي ستوفرها للقطاع الحكومي G2G.	100 %	8.57 %	9.0 %
نسبة الخدمات التي وفرتها الحكومة الإلكترونية ضمن قناة الخدمات العامة.	100 %	25 %	25 %
نسبة المؤسسات الحكومية المرتبطة بشبكة المعلومات الوطنية.	100 %	100 %	100 %

نسبة المؤسسات الحكومية المرتبطة بشبكة الانترنيت.	100 %	100 %	100 %
نسبة المؤسسات الحكومية التي أودعت بياناتها في مراكز المعلومات.	100 %	…	…

ولا زال قطاع الصحة الالكترونية بعيداً جداً عن تحقيق الأهداف المرسومة له في جميع مفاصل أنشطته وخدماته، أنظر الجدول (3 - 8). فلا زال مشروع البطاقة الصحية السيبرانية غائباً بالكلية عن أرض الواقع، وكذلك الحال بالنسبة لاستخدام الأطباء لنظام الوصفة الالكترونية.

بينما لا زال العمل مستمراً على استكمال ربط المراكز الصحية في المدن الكبيرة والأرياف بشبكة المعلومات المحلية، وشبكة الانترنيت، بيد أن نسب التقدم على أرض الواقع ما انفكت بعيدة جداً عن الأهداف المرجوة.

الجدول (3 - 8) ـ الأهداف المرسومة لخطط تطوير منظومة الصحة الالكترونية ـ الخمسية في إيران (2009-2014).

الهدف	الغاية المرجوة عند نهاية الخطة	الحالة في عام 2014	نسب الانجاز
نسبة السكان الذين يمتلكون ملفات سجلات صحية ـ رقمية.	100 %	4 %	4 %
نسبة المراكز الصحية المرتبطة بشبكة المعلومات الوطنية.	60 %	8900مركز	…
نسبة المراكز الصحية التي تمتلك نظم معلومات مرخصة.	80 %	173مركز	…
نسبة المواطنين الذين يمتلكون بطاقة تأمين صحي ـ ذكية.	30 %	…	…
نسبة الأطباء الذين يستخدمون نظام الوصفة الالكترونية.	15 %	…	…

المصدر: ***M.O.ICT,2015***

وقد حقق نظام التعليم الالكتروني قفزة نوعية في الفضاء السيبراني الإيراني، فتجاوز عتبة الأهداف المرسومة بنسب كبيرة ـ أنظر الجدول (3 - 9). فحصلت طفرة على صعيد مؤشر التعليم الالكتروني (نسبة النمو 131 %)، ونسبة المدرسين الذين يستخدمون الحاسب في المدارس (نسبة النمو 500 %)، ونسبة الأساتذة الجامعيين الذين يستخدمون الحاسب (نسبة النمو 156 %).

وكان للمناهج التعليمية حصة جيدة على صعيد استخدام أدوات التعليم الالكتروني في المدارس (نسبة النمو 240 %)، بينما بلغت نسبتها في الجامعات والمعاهد العليا 133 %. وتقدمت المدارس على الجامعات في اعتمادها على نظم التعليم الالكتروني، فبلغت النسبة لدى الأولى 300 % بينما لم تزد نسبتها لدى الثانية على 33 %.

الجدول (3 - 9) ـ الأهداف المرسومة لخطط تطوير منظومة التعليم الالكتروني ـ الخمسية في إيران (2009-2014).

الهدف	الغاية المرجوة عند نهاية الخطة	الحالة في عام 2014	نسب الانجاز
مؤشر التعليم الالكتروني.	30 %	39.8 %	131 %
نسبة المدرسين الذين يستخدمون الحاسب في المدارس لأغراض تعليمية.	10 %	50 %	500 %
نسبة الأساتذة الجامعيين الذين يستخدمون الحاسب في المدارس لأغراض تعليمية.	45 %	70 %	156 %
نسبة المناهج الدراسية التي تستخدم أدوات التعليم الالكتروني بالمدارس.	25 %	60 %	240 %
نسبة المناهج الدراسية التي تستخدم أدوات التعليم الالكتروني بالجامعات والمعاهد العليا.	30 %	40 %	133 %
نسبة المدارس التي تعتمد نظم التعليم الالكتروني.	20 %	60 %	300 %
نسبة الجامعات التي تعتمد نظم التعليم الالكتروني.	30 %	10 %	33 %

المصدر: ***M.O.ICT,2015***

ولم تفلح أنشطة الاقتصاد الالكتروني في إيران بتحقيق نجاحات ملموسة على أرض الواقع، فتباعد الواقع كثيراً عن الأهداف المرسومة ـ أنظر الجدول (3 - 10).

الجدول (3 - 10) ـ الأهداف المرسومة لخطط تطوير اقتصاد تقنيات المعلومات والاتصالات ـ الخمسية في إيران (2009-2014).

الهدف	الغاية المرجوة عند نهاية الخطة	الحالة في عام 2014	نسب الانجاز
نسبة سلع وخدمات المعلومات والاتصالات المصدّرة منسوبة الى حجم التصدير غير المشمول بمنتجات النفط.	15 %	0.146 %	10 %
حصة قطاع المعلومات والاتصالات من الناتج الإجمالي المحلي.	2 %	...	0 %

المصدر: ***M.O.ICT,2015***

أما على صعيد البحث والتطوير في قطاع المعلومات والاتصالات، فقد نجحت الحكومة في توفير الخدمات السيبرانية الداعمة لأنشطتها، بيد أنها لم تفلح في توفير التمويل الكافي لدعم أنشطتها البحثية، مع عدم كفاية أعدادها لتلبية الاحتياجات المتزايدة للقطاع الحكومي، والقطاع الخاص ـ أنظر الجدول (3 - 11).

الجدول (3 - 11) ـ الأهداف المرسومة لخطط البحث والتطوير قطاع تقنيات المعلومات والاتصالات ـ الخمسية في إيران (2009-2014).

الهدف	الغاية المرجوة عند نهاية الخطة	الحالة في عام 2014	نسب الانجاز
نسبة ميزانية بحوث قطاع تقنيات المعلومات والاتصالات من الناتج الإجمالي المحلي الإيراني.	2 %	...	0 %
نسبة ميزانية بحوث قطاع تقنيات المعلومات والاتصالات من الميزانية الوطنية المخصصة لعموم أنشطة البحث والتطوير.	3 %	...	0 %
نسبة عدد البحوث المنجزة في قطاع المعلومات والاتصالات والمسجلة في معهد إيران العلمي منسوبة الى عدد البحوث الكلية.	5 %	8.5 %	171 %
نسبة مراكز البحث والتطوير العلمي ـ العامة التي تمتلك خدمة انترنيت عريضة.	100 %	100 %	100 %
عدد مراكز البحث والتطوير العلمي ـ العامة التي ترتبط بشبكة المعلومات الوطنية.	100	16مركز	...

المصدر: ***M.O.ICT,2015***

ولا زالت صناعة المحتوى السيبراني الإيراني متراجعة عن الأهداف المرسومة لها، فهناك تراجع في نسبة المطبوعات السيبرانية، وعدد الكتب الالكترونية المنشورة، وحجم المحتوى السيبراني الموثّق بشكل ملحوظ عند مقارنة ما تحقق بالأهداف المرسومة، أنظر الجدول (3 - 12).

ويمكن أن يعزى ذلك الى الضغط الذي تمارسه نظم الرقابة الصارمة، والمتابعة المستمرة لتفاصيل الخطاب المطروح على مواقع الانترنيت، بالإضافة الى الحظر على مواقع المدونات السيبرانية، وموسوعات ويكي التعاونية، وشبكات التواصل الاجتماعي، الأمر الذي جعل جزءاً كبيراً من المحتوى السيبراني مرتبطاً بنشاط المؤسسات الحكومية، والذي لا يرقى الى المستوى المطلوب.

الجدول (3 - 12) ـ الأهداف المرسومة لخطط تطوير المحتوى السيبراني الثقافي والإسلامي الايراني ـ الخمسية في إيران (2009-2014).

الهدف	الغاية المرجوة عند نهاية الخطة	الحالة في عام 2014	نسب الانجاز
نسبة المطبوعات السيبرانية الى المطبوعات الكلية في إيران.	10 %	0.2 %	2 %
نسبة الكتب الالكترونية المنشورة الى عدد الكتب الكلية المنشورة.	10 %	0.2 %	2 %
نسبة المجلات والجرائد الالكترونية المطبوعة الى التقليدية.	10 %	26.6 %	266 %
نسبة شبكات التواصل الاجتماعي الإيرانية والفارسية.	10 %	3.09 %	30.9 %
نسبة المحتوى السيبراني الموثّق الى المحتوى المعرفي الكلي الإيراني (كتب، مجلات، جرائد، وأفلام).	15 %	0.35 %	2 %

المصدر: ***M.O.ICT,2015.***

ويظهر من الجدول (3 - 13) أن القضاء الإيراني يبذل جهوداً حثيثة لتطوير منظومته السيبرانية، والسعي لبلوغ الأهداف المرسومة له، والتي قاربت حوالي 85 % من النسب التي خطط لتنفيذها خلال السنوات 2009-2014.

الجدول (3 - 13) ـ الأهداف المرسومة لخطط تطوير منظومة القضاء الالكترونية ـ الخمسية في إيران (2009-2014).

الهدف	الغاية المرجوة عند نهاية الخطة	الحالة في عام 2014	نسب الانجاز
نسبة السجلات القضائية الالكترونية الى السجلات القضائية الكلية.	100 %	85 %	85 %
نسبة الخدمات القضائية ـ الالكترونية.	100 %	14خدمة	...

المصدر: ***M.O.ICT,2015***

وقبل أن ننتقل الى الفقرة التالية، سنحاول مراجعة مؤشرات نمو قطاع المعلومات والاتصالات بإيران والمرتبة التي نجحت ببلوغها بعد أن أنضجت رؤيتها وسياستها على أرض الواقع وفق معطيات عام 2015 ـ أنظر الجدول **(3 - 14).**

ويبدو واضحاً أن هناك الكثير من العمل والجهد الاستثنائي الذي يقع على عاتق الجهات التنفيذية في قطاع المعلومات والاتصالات الإيراني، ذلك لأن ما تم تحقيقه على أرض الواقع في عام 2015 يؤكد تراجع إيران ضمن قائمة مؤشرات قطاع المعلومات والاتصالات العولمي.

فلا زالت مؤشرات: نمو أدوات المعلومات والاتصالات، وتطور الحكومة الالكترونية، الجاهزية الشبكاتية، وامن المعلومات العولمي، والتنافسية العولمية، وسلة أدوات المعلومات والاتصالات متراجعة بالمقارنة مع دول المنطقة (وبالخصوص الدول الخليجية وتركيا)، وعلى المستوى العولمي.

ويعد هذا التراجع مؤشراً واضحاً على عدم كفاية التخصيصات المالية لتلبية احتياجات هذا القطاع، مع وجود حاجة اكيدة لتنمية القطاع من خلال زج تقنيات جديدة بعد التخلص من الحصار التقني المفروض على البلاد، وبناء القدرات البشرية خارج نطاق المدن الكبيرة، والتقليل من كلفة سلة الخدمات السيبرانية والاتصالية، والتقليل من وطأة المراقبة والحظر على مواقع فضاء الانترنيت، واستبعاد الحضور القاهر لسياسة النظام وثقافته عن فضاء الانترنيت المحايد.

الجدول (3 - 14) ـ مؤشرات النمو في قطاع المعلومات والاتصالات بإيران وفق المعايير العالمية ـ عام 2015.

دليل التقييم الدولي	الجهة	دليل المرتبة الأولى	المتوسط العولمي	دليل إيران	مرتبة إيران
دليل نمو أدوات المعلومات والاتصالات IDI.	ITU	8.86	4.77	4.29	94
دليل تطور الحكومة الالكترونية EGDI.	UN	0.9642	0.4712	0.4508	105
دليل الجاهزية الشبكاتية NRI.	World Economic Forum	6	4.07	3.06	96
دليل أمن المعلومات العولمي GCI.	ABI Research	0.824	0.284	0.294	19
دليل التنافسية العولمي.	World Economic Forum	5.70	4.21	4.03	83
دليل سلة أدوات المعلومات والاتصالات IPB.	ITU	0.2	9.04	0.6	12

المصدر: ***I.I.S.,2015.***

3 . 2 . توافق سياسة المعلومات الوطنية مع أهداف المؤتمر العالمي لمجتمع المعلومات:

رغم حرص إيران على تشكيل جميع تفاصيل رؤيتها وسياستها السيبرانية دون أي تأثير خارجي قد يؤثر بصورة مباشرة، أو غير مباشرة على خطاطة الثورة الإسلامية وثقافتها المميزة، إلا أنها تولي اهتماماً بالالتحاق بمعايير وأهداف المؤتمر العالمي لمجتمع المعلومات WSIS لكي تضمن توافق حضورها العولمي مع المعايير الدولية، مع ضمان ميزاتها التنافسية بين بلدان المنطقة، وعلى المستوى العولمي من خلال تحقيق هذه الأهداف على أرض الواقع والارتقاء بواقع الفضاء السيبراني والاتصالات الإيراني.

لقد وضعت الإدارة المشرفة على المؤتمر العالمي لمجتمع المعلومات عشرة أهداف ينبغي على الدول بلوغها عند عام 2015، لضمان حسن انتمائها لمجتمع المعلومات المعاصر. وشملت هذه الأهداف التزامها بتنفيذ مجموعة متنوعة من الإنجازات على صعيد: البنية التحتية للمعلومات والاتصالات، وربط المساكن بأدوات المعلومات والاتصالات، والارتقاء بمستوى الأفراد على صعيد استخدام هذه الأدوات، وكذلك القطاع الحكومي، وقطاع التجارة والأعمال. مع تطوير حضور واستخدام أدوات المعلومات والاتصالات في النظام التعليمي، وترسيخ التجارة وتوفير الخدمات ذات الصلة بأدوات المعلومات والاتصالات.

وقد عكفت كوادر الاتحاد الدولي للاتصالات *ITU* على إعداد الخطاطة الإحصائية لتحديد مستوى تحقيق الأهداف التي تبناها المؤتمر العالمي، والتي تلقفتها منظمة تقنية المعلومات الإيرانية *ITO* وقامت بإجراء مسوحات ميدانية لاستقصاء وجمع وتحليل البيانات من بيئة مجتمع المعلومات الإيراني، وبالتعاون المباشر مع المركز الاحصائي في إيران *Statistical Center of Iran*، والتي لم تفلح بالحصول على جميع البيانات المطلوبة لتقييم أداء وزارة تقنيات المعلومات والاتصالات الإيرانية، مما أجبرها على تعويض نقص البيانات الميدانية من بيانات توفرت لدى المؤسسات الدولية، مثل: اليونسكو، والاتحاد الدولي للاتصالات (*I.T.O.,2015*).

لذا جاءت البيانات من موارد متعددة، فاختلط الواقع الميداني في إيران مع الإحصاءات الدولية، والتي قد لا تتطابق مع الواقع في أحيان كثيرة، بالتقارب أو التباعد، نتيجة اعتمادها على نهج تقريب، أو احصائيات لا تلتصق بالنسيج الحقيقي للواقع.

وسنحاول مراجعة نضوج واقع أدوات المعلومات والاتصالات وتقنياتها، في إيران، خلال السنوات 2012-2014 لبلوغ الأهداف مع إطلالة عام 2015، بحسب تسلسل الأهداف التي تبنتها إدارة المؤتمر العالمي لمجتمع المعلومات:

يظهر في الجدول (3 - 15) ما نجحت إيران في تحقيقه من الهدف الأول، والذي تضمن ربط جميع القرى الإيرانية بأدوات المعلومات والاتصالات مع إنشاء نقاط تتيح للمجتمع الإيراني الوصول الى موارد المعلومات وخدمات شبكة الانترنيت.

الجدول (3 - 15) ـ مستويات تحقيق مؤشرات بلوغ الهدف الأول من أهداف المؤتمر العالمي لمجتمع المعلومات.

المؤشر	ما تم تحقيقه خلال السنوات 2012-2014		
	2012	2013	2014
نسبة سكان الريف الذين تشملهم تغطية الهاتف المحمول.	...	69.7 %	71.7 %
نسبة المساكن التي تمتلك هاتفاً أرضياً.	...	97.6 %	...
نسبة المساكن التي تتمتع بالارتباط مع خدمة الانترنيت.	...	37.8 %	42.9 %
نسبة المواطنين الذين يستخدمون الانترنيت.	26.0 %	31.4 %	35.1 %
نسبة المساكن التي تمتلك حاسباً.	...	45.9 %	52.0 %

المصدر: *M.o.ICT,2015*

ويشمل الهدف الثاني للمؤتمر العالمي، مراجعة مستوى ارتباط مدارس التعليم الأساسي الابتدائية والثانوية بخدمة الانترنيت وتوفر فرصة وصول طلبتها الى هذه الخدمة. ويبدو من الجدول (3 - 16) أن وزارة التعليم في إيران لا زالت بعيدة عن تحقيق مضامين هذه المرحلة، ولا زالت الكثير من المدارس محرومة من الارتباط بخدمة الانترنيت، و/أو تتوفر لديها البنية التحتية لتحقيق هذا الهدف.

الجدول (3 - 16) ـ مستويات تحقيق مؤشرات بلوغ الهدف الثاني من أهداف المؤتمر العالمي لمجتمع المعلومات.

المؤشر	ما تم تحقيقه خلال السنوات 2012-2014		
	2012	2013	2014
نسبة عدد الطلبة للحاسب الواحد.	19.4	23.5	30
نسبة المدارس التي تمتلك ارتباطاً بخدمة الانترنيت.	50.7 %	51.7 %	55.0 %

المصدر: ***M.o.ICT,2015***

وتضمن الهدف الثالث تقييم مستوى ارتباط جميع مراكز العلوم ومراكز البحث العلمي في البلاد بأدوات المعلومات والاتصالات، وتوفير بيئة مناسبة لاستثمار المحتوى العلمي والتقني المطروح على شبكة الانترنيت وشبكات المعلومات المحلية. ويبدو واضحاً من الجدول (3 - 17) أن كل من وزارة العلوم والبحوث والتقنية، وبالتنسيق مع منظمة إيران لتقنية المعلومات قد حققت تقدماً ملموساً على ربط هذه المراكز بخدمة الانترنيت العريضة، مع توفير ارتباط مستدام مع الشبكة الوطنية للبحث والتعليم، بيد أن ربط محتوى هذه الشبكة مع الانترنيت لا زال متراجعاً الى حد كبير.

الجدول (3 - 17) ـ مستويات تحقيق مؤشرات بلوغ الهدف الثالث من أهداف المؤتمر العالمي لمجتمع المعلومات.

المؤشر	ما تم تحقيقه خلال السنوات 2012-2014		
	2012	2013	2014
نسبة مراكز العلوم والبحث العامة المرتبطة بخدمة الانترنيت العريضة.	100 %	100 %	100 %
وجود ارتباط مستدام مع الشبكة الوطنية للبحث والتعليم.	...	نعم	نعم
نسبة مراكز العلوم والبحث العامة التي ترتبط فيها الشبكة الوطنية للبحث والتعليم مع خدمة الانترنيت.	2.5 %	3.85 %	...

المصدر: ***M.o.ICT,2015***

أما بالنسبة للهدف الرابع، فقد ركز الاهتمام على ربط المكتبات العامة، والمتاحف، ومكاتب البريد، ومراكز الأرشيف الحكومي بأدوات المعلومات والاتصالات. وقد نهضت بهذه المهمة إدارات هذه المؤسسات بالتنسيق مع وزارة أدوات المعلومات والاتصالات الإيرانية. ويبدو واضحاً من الجدول (3 - 18) أن هناك تقدماً ملموساً في بعض عناصر هذا

الهدف، بينما لا زالت المكتبات العامة، ومراكز الأرشيف الحكومي بعيدة عن تحقيق التزاماتها المتضمنة في تفاصيل هذا الهدف.

الجدول (3 - 18) ـ مستويات تحقيق مؤشرات بلوغ الهدف الرابع من أهداف المؤتمر العالمي لمجتمع المعلومات.

المؤشر	ما تم تحقيقه خلال السنوات 2012-2014		
	2012	2013	2014
نسبة المكتبات العامة التي ترتبط بخدمة الانترنيت العريضة.	49.9 %	76.2 %	82.0 %
نسبة المكتبات العامة التي توفر نقاط ارتباط عامة بالإنترنيت.	45.3 %	51.7 %	…
نسبة المكتبات العامة التي تمتلك مواقع ويب.	…	29.4 %	37.0 %
نسبة المتاحف التي ترتبط بخدمة الانترنيت العريضة.	30 %	63 %	71 %
نسبة المتاحف التي تمتلك مواقع ويب.	10 %	39 %	…
نسبة مكاتب البريد التي ترتبط بخدمة الانترنيت العريضة.	90.2 %	90.4 %	93.0 %
نسبة مكاتب البريد التي توفر نقاط وصول عامة للانترنيت.	0	0	…
عدد مؤسسات الأرشيف الوطني التي ترتبط بخدمة الانترنيت العريضة.	100	100	100
عدد مؤسسات الأرشيف الوطني التي تمتلك مواقع ويب.	100	100	100
نسبة الأرشيف الذي تم تحويله الى محتوى رقمي.	8.35 %	20.0 %	32.0 %
نسبة المحتوى السيبراني للأرشيف المتوفر للتداول العام.	6.26 %	9.0 %	14.4 %

المصدر: *M.o.ICT,2015*

وتضمن الهدف الخامس للمؤتمر العالمي تقييم مستوى ارتباط المؤسسات الصحية (المستشفيات، والمراكز الصحية) بأدوات المعلومات والاتصالات. ويبدو واضحاً من الجدول الخاص بتنفيذ عناصر هذا الهدف ـ أنظر الجدول (3 - 19)، أن المؤسسات الصحية الإيرانية، المتفوقة على صعيد المهارات الطبية في المنطقة، قد نجحت بتحقيق جل التزاماتها باستثناء توفير بيئة ارتباط لكوادرها الطبية بخدمة الانترنيت، واخفاق الحكومة في ربط الخدمات الطبية مع منظومتها السيبرانية.

الجدول (3 - 19) ـ مستويات تحقيق مؤشرات بلوغ الهدف الخامس من أهداف المؤتمر العالمي لمجتمع المعلومات.

المؤشر	ما تم تحقيقه خلال السنوات 2012-2014		
	2012	2013	2014
نسبة المستشفيات العامة المرتبطة بخدمة الانترنيت العريضة.	…	100 %	100 %
نسبة المراكز الصحية المرتبطة بخدمة الانترنيت العريضة.	…	90 %	97 %
مستوى توظيف الحواسب والانترنيت في إدارة صحة المرضى.	…	3.1 مليون وثيقة مريض	…

المصدر: *M.o.ICT,2015*

وشمل الهدف السادس تقييم مستوى الحوكمة السيبرانية لمؤسسات الدولة المركزية، بمختلف اختصاصاتها، مع إنشاء مواقع ويب للتواصل مع المواطن وتوفير خدمات الكترونية. ويبدو واضحاً من الجدول (3 - 20) أن الحكومة الإيرانية قد نجحت في زج تقنيات المعلومات والاتصالات في جل مفاصل أقسامها المختلفة، وحققت التزاماتها، بينما لم تنجح في تحويل الاستخدام الروتيني لموظفيها عبر شبكة الانترنيت، من جهة، وفي تطوير عملية إيصال الخدمة السيبرانية للمواطنين عبر الشبكة.

الجدول (3 - 20) ـ مستويات تحقيق مؤشرات بلوغ الهدف السادس من أهداف المؤتمر العالمي لمجتمع المعلومات.

المؤشر	ما تم تحقيقه خلال السنوات 2014-2012		
	2012	2013	2014
نسبة موظفي الحكومة المركزية الذين يتعاملون باستمرار مع الحاسب.	...	73 %	90 %
نسبة موظفي الحكومة المركزية الذين يستخدمون الانترنيت باستمرار.	...	60 %	...
نسبة مؤسسات الدولة التي تمتلك شبكة معلومات محلية.	100 %	100 %	100 %
نسبة مؤسسات الدولة التي تمتلك شبكة Intranet.	100 %	100 %	100 %
نسبة مؤسسات الدولة التي ترتبط بشبكة الانترنيت.	100 %	100 %	100 %
نسبة مؤسسات الدولة التي تمتلك موقع ويب.	100 %	100 %	100 %
مستوى تطور الخدمات السيبرانية للتواصل بالخدمات مع الغير.	...	25 %	39 %

المصدر: *M.o.ICT,2015*

وشمل الهدف السابع من أهداف المؤتمر العالمي تكييف المناهج الدراسية في مراحل التعليم الابتدائي والثانوي مع التحديات التي يفرضها مجتمع المعلومات، مع الأخذ بنظر الاعتبار خصائص البيئة المحلية في إيران.

ويبدو واضحاً من الجدول (3 - 21) أن مناهج التعليم الأساسي في إيران لا زالت قاصرة عن بلوغ هذا الهدف، لأن جل ما حققته من نسب انجاز على أرض الواقع لم ترق الى 45 % من النسب المخطط لها.

الجدول (3 - 21) ـ مستويات تحقيق مؤشرات بلوغ الهدف السابع من أهداف المؤتمر العالمي لمجتمع المعلومات.

المؤشر	ما تم تحقيقه خلال السنوات 2012-2014		
	2012	2013	2014
نسبة المدرسين المتخصصين بتقنية المعلومات في المدارس.	28.0 %	38.5 %	50.0 %
نسبة المدرسين الذين تدربوا على التدريس بواسطة أدوات المعلومات.	9.3 %	17.7 %	35.0 %
نسبة المدارس التي تستخدم مناهج مدعمة بالحاسب.	21.4 %	20.7 %	30.0 %
نسبة المدارس التي تستخدم مناهج مدعمة بالإنترنيت.	15.8 %	20.7 %	30.0 %

المصدر: *M.o.ICT,2015*

وقد أوكلت مهمة النهوض بواقع التعليم الأساسي (للتكيف مع متطلبات مجتمع المعلومات) على عاتق وزارة التربية، والتي لا زالت مثقلة بالتحديات التي تضغط عليها نتيجة لتوسع رقعة التعليم الأساسي، وشحة الكوادر المهنية، والموارد الداعمة للعملية التدريسية، وغيرها من التحديات التي ستشكل عقبة أمام تحقيق عناصر هذا الهدف في وقت قريب.

أما الهدف الثامن فتضمن جملة من المعايير التي تهتم بحضور وسائل الإعلام السمعية والمرئية في مسكن المواطن الإيراني. ويظهر من البيانات التي توفرت مركز إيران للإحصاء، أن نسبة المساكن التي تمتلك جهاز راديو لم تتجاوز 57 %، في حين بلغت نسبة المساكن التي تمتلك جهاز التلفاز حوالي 98.4 %، أما توفر قنوات تلفزيونية متعددة بالمساكن فقد بلغت نسبتها حوالي 0 %.

وبالنسبة للهدف التاسع فيعنى بتقييم مستوى توظيف اللغة في إنتاج المحتوى السيبراني، وأساليب التعامل مع اللغات العالمية أثناء استخدام شبكة الانترنيت (*I.T.O.,2015*).

ويضم الجدول (3 - 22) بعض البيانات التي تخص عناصر هذا الهدف، والتي تؤشر بجلاء الى وجود حاجة ماسة الى تطوير المحتوى السيبراني الإيراني، وتوسيع دائرة الحضور اللغوي الفارسي على الانترنيت، وتطوير العنونة الالكترونية للمواقع الإيرانية بمختلف مستوياتها.

الجدول (3 - 22) ـ مستويات تحقيق مؤشرات بلوغ الهدف التاسع من أهداف المؤتمر العالمي لمجتمع المعلومات.

المؤشر	ما تم تحقيقه خلال السنوات 2012-2014		
	2012	2013	2014
نسبة استخدام اللغة الفارسية على الانترنيت.	21.0 %	26.0 %	31.4 %
نسبة المواقع باللغة الفارسية.	…	0.8 %	0.9 %
عدد المواقع المسجلة بالنطاق العولمي.	166.1	166.1	…
عدد المقالات المدونة في موقع *Wikipedia*.	200,000	300,000	400,000

المصدر: *M.o.ICT,2015*

وكان الهدف العاشر، والأخير، للمؤتمر العالمي هو ضمان أن أكثر من نصف سكان الكرة الأرضية يتمتعون بفرصة الوصول الى أدوات المعلومات والاتصالات، واستثمار موارد المعلومات المطروحة في فضاء الانترنيت. وقد حدد لتقييم بلوغ هذا الهدف جملة من المعايير التي روجعت قيمها على أرض إيران، فكانت النتائج كما هو في الجدول (3 - 23).

الجدول (3 - 23) ـ مستويات تحقيق مؤشرات بلوغ الهدف العاشر من أهداف المؤتمر العالمي لمجتمع المعلومات.

المؤشر	ما تم تحقيقه خلال السنوات 2012-2014		
	2012	2013	2014
عدد المشتركين بخدمة الهاتف المحمول/100 مواطن.	76.1	85.0	91.0
نسبة المساكن التي تمتلك هاتفاً أرضياً.	…	97.1 %	…
نسبة المواطنين الذين يستخدمون الهاتف المحمول.	…	61.5 %	71.7 %
نسبة المواطنين الذين يستخدمون الانترنيت.	26 %	31.4 %	35.1 %
نسبة المساكن المرتبطة بخدمة الانترنيت.	…	37.8 %	42.9 %

المصدر: *M.o.ICT,2015*

ويبدو واضحاً أن إيران قد نجحت بتحقيق الهدف العاشر على صعيد الخدمات الهاتفية (الأرضية والمحمولة)، بينما أخفقت في بلوغ حافات الهدف العاشر على صعيد الانترنيت (الوفرة والاستخدام) والتي لم تصل نسب المتحقق منها أكثر من 42 % في أفضل الأحوال.

4 . الحكومة الالكترونية في إيران:

اعتمد نظام الحكومة الالكترونية الإيرانية مبدأ استخدام تقنيات، وأدوات المعلومات والاتصالات، والنظم البرمجية في إنشاء حزمة متنوعة من التطبيقات التي جعلت من فضاء مواقع الويب منطلقاً لطرح خدمات حكومية لمؤسساتها وشركائها، ولقطاع التجارة والأعمال، والمواطنين. وتهدف هذه الخدمات الى توطيد الصلة بين الحكومة وشركائها، والمواطنين، وبقية قطاعات المجتمع، من خلال قنوات رقمية تذلل العقبات أمام عمليات التواصل مع تحسين فضاء تداول المعلومات، وتوفير البيانات، وإيصال الخدمات لمختلف فئات زبائنها.

تنتمي الطبقة الأولى لحفريات الحكومة الالكترونية في إيران الى بدايات تشكيل الخطة الوطنية لتطوير استخدام المعلومات وتقنية الاتصالات في إيران، والذي أطلق عليها اسم *TAKFA*[71]. أعدت هذه الخطة الطموحة في أروقة منظمة الإدارة والتخطيط *Management & Planning Organization* في بدايات عام 2000، وظفرت بمصادقة مجلس الوزراء في منتصف العام ذاته، قبل أن تحال الخطة الى المؤسسات التنفيذية لكي يباشر بالعمل على ترجمتها على الفضاء السيبراني الايراني (*Atashak&Mahzadeh,2008*).

لم تقتصر هذه الخطة على مشروع الحكومة الالكترونية، وإنما تضمنت ستة قطاعات أخرى داعمة لإنجاح مشروع الحكومة الالكترونية وخدماتها شملت: توسيع تطبيقات تقنية المعلومات في العملية التعليمية والتدريب وبناء القدرات والمهارات السيبرانية لدى الموارد البشرية الايرانية، وتوسيع دائرة تطبيقات تقنية المعلومات لتحسين الخدمات الاجتماعية، وتطوير التطبيقات السيبرانية في ميادين الثقافة والفنون وترسيخ حضور اللغة الإيرانية في فضاء الانترنيت، وتطوير التطبيقات السيبرانية في مجال الاقتصاد والتجارة الالكترونية وقطاع التجارة والأعمال، وأخيراً توسيع حضور تقنيات المعلومات وتطبيقاتها لدى المؤسسات الصغيرة والمتوسطة *SME's* (*Atashak&Mahzadeh,2009*).

وتبين من مراجعة وثائق خطة الحكومة الالكترونية في إيران أنها قد توجهت نحو تحقيق تسعة أهداف وترسيخ حضورها في البيئة السيبرانية الوطنية، شملت (*Atashak&Mahzadeh,2008*):

1. إدارة وإصدار التشريعات اللازمة لضمان مستوى أمني رصين لمحتوى شبكات الحكومة الافتراضية ـ الخاصة *VPN* وإيصال مادة فيضها السيبراني الى صنّاع القرار بمنأى عن عمليات الاختراق أو التشويش.
2. توفير التمويل اللازم لميكنة نظم التخطيط والموازنة المالية، وتصميم نظم لتقارير الكلفة، وتقييم الأداء، وتخصيصات الائتمان.
3. ميكنة موارد الدخل القومي، واستكمال توطين نظام المحاسبة المالية في الفضاء السيبراني الوطني لدعم نشاط عمل وزارة الشؤون الاقتصادية والمالية.
4. ميكنة نظام المرور وإدارة حركة المركبات في البلاد وتوفير قواعد بيانات متكاملة لإدارة هذه المنظومة مع تقديم خدمات آنية للمواطنين.

[71] . تضمنت رسالة مشروع *TAKFA* وغايتها أن تزداد وتتعمق مكانة إيران في مجال ترسيخ مواردها المعرفية وتطوير آلة اقتصادها السيبراني، والارتقاء بميزاتها التنافسية، في القرن الحادي والعشرين من خلال الاستخدام الرشيد لتقنية المعلومات والاتصالات، وأدواتها، وتطبيقاتها (*Atashak&Mahzadeh,2009*).

5. إنشاء مواقع ويب للمؤسسات الحكومية تحتوي على قواعد بيانات عن الخدمات الحكومية لضمان إيصال الخدمات للمواطنين، وتصميم نماذج الكترونية e-Forms يسهل التعامل معها من قبل المواطنين للحصول على الدعم الذي يرومون الحصول عليه عند دخولهم الى بوابات مواقع الويب الحكومية.
6. إعداد مسودة القوانين والخطط المناسبة لإدارة الحضور السيبراني للمؤسسات والشركات، والأفراد في فضاء الانترنيت على المستوى الوطني، والتأكيد على قانون مواجهة الجرائم السيبرانية، وحماية الملكية الفكرية للمحتوى السيبراني، وتطوير نظام التوقيع السيبراني.
7. ترسيخ عناصر البنية التحتية الوطنية للمعلومات والاتصالات وتوسيع قنوات الاتصال السيبراني السريع *Information High Ways* وبمشاركة مباشرة من قبل وزارة المعلومات والاتصالات، وفي ضوء المعايير المعتمدة دولياً، وتلك التي قد وقع عليها اختيار مجالس وهيئات المعلومات الوطنية للتوافق مع خطاطة الثورة الاسلامية وغاياتها.
8. إنشاء بوابات رقمية ـ حكومية تتكامل من خلالها عملية حضور مواقع الويب الحكومية وتتكامل مع عملية توفير الخدمات السيبرانية للمواطنين، والجهات المستفيدة منها.
9. إعداد الخطط الرئيسة لقطاع المعلومات والاتصالات على المستويات الوطنية، والقطاعية، والإقليمية لتوضيح تفاصيل المشهد السيبراني لفضاء معلومات الحكومة الالكترونية ومتطلبات إدارة وتوزيع خدماتها بشكل متوازن على عموم رقعة الفضاء الإيراني.

منذ أن أطلق مشروع الحكومة الالكترونية في بداية الألفية الجديدة، ضمن ملف خطة *TAKFA* والمؤسسات الحكومية تسارع في عملية الالتحاق بفضائه السيبراني، الذي بدأ بالتوسع تدريجياً، وبوتائر بطيئة نتيجة للعقبات المقيمة على خارطة طريق المشروع ـ أنظر الجدول (3 -).

الجدول (3 - 24) ـ التطورات الحاصلة في المؤسسات الحكومية الإيرانية على صعيد ارتباطها بفضاء الحكومة الالكترونية خلال السنوات 2004-2009.

النشاط	عدد المؤسسات المرتبطة بفضاء الحكومة الالكترونية الايرانية					
	2004	2005	2006	2007	2008	2009
مؤسسات حكومية تمتلك نظم عامة مميكنة.	5	166	27	38	49	60
مؤسسات حكومية تمتلك نظم خاصة مميكنة.	1	5	9	13	17	20
مؤسسات حكومية لديها حضور على مواقع الويب.	20	36	52	68	84	100
مؤسسات حكومية تملك مواقع ويب تفاعلية.	0	5	9	13	17	20
مؤسسات حكومية توفر خدمات إلكترونية.	0	3	6	9	12	15

المصدر: *I.I.S.,2015*.

ويبدو واضحاً أن ما تحقق خلال السنوات 2004-2009 يعد متواضعاً بالمقارنة مع امتدادات وحجم حضور المؤسسات الحكومية الإيرانية على أرض الواقع الإيراني. ويمكن أن يعزى هذا الأمر الى شحة التخصيصات الحكومية من جهة، ووجود محددات وإجراءات حجب على المحتوى تقف عائقاً، في كثير من الأحيان أمام إنشاء مواقع الويب، وتوفير خدمات تفاعلية فيها، بالإضافة الى ارتفاع كلفة سلة خدمات الانترنيت في البلاد.

تستقر الحكومة الالكترونية الإيرانية وفق مؤشر تطوّر الحكومات الالكترونية لعام 2014 ضمن المجال المتوسط (حيث تتراوح قيمة المؤشر بين 0.25-0.50) وتشترك معها في المجال ذاته من دول المنطقة: سورية، والعراق، وباكستان، وتركمنستان (*UN,2014*).

وقد بلغت قيمة هذا المؤشر لديها 0.4508، أما قيمة عناصر هذا المؤشر فبلغت: 0.3701 على صعيد الخدمات الالكترونية، 0.2904 على صعيد البنية التحتية الاتصالية، بينما حققت قيمة عالية في عنصر الموارد البشرية بعد أن بلغت قيمته 0.6882. ويلاحظ تراجع قيمة المؤشر الإيراني قبالة متوسط قيمته في قارة آسيا (0.4951)، والمتوسط العولمي (0.4712)، وكذلك الحال بالنسبة لعنصري الخدمات الالكترونية (0.3919)، والبنية التحتية الاتصالية (0.3650)، بينما نجحت في تجاوز المتوسط العولمي، وبفارق بسيط، على صعيد عنصر الموارد البشرية (0.6566) (*UN,2014*).

لقد أظهرت الدراسة التي قام بها (*Borna&Seifloo,2015*) ، بجلاء، أن الحكومة الإلكترونية في إيران لا زالت بعيد عن مرحلة النضوج، رغم الجهود الحثيثة التي بذلت في نهاية المدة الرئاسية لأحمدي نجاد، والدعم غير المسبوق الذي توفره الإدارة الحكومية للرئيس روحاني.

فالبيئة التحتية الحاضنة للحكومة الالكترونية، والتطبيقات التي تقيم في مواقع ويب الخدمات التي توفرها لزبائنها، لا زالت بحاجة الى جهد كبير لتعزيزها. وبالوقت ذاته لا زالت سرعة خدمة الانترنيت متواضعة نتيجة لعدم كفاية سعة الحزمة السيبرانية، إضافة الى عقبة المراقبة والحظر والتي تسهم في تباطؤ سرعة الخدمة، وتثبيط الكثير من الخدمات السيبرانية.

يضاف الى كل هذا ميل الإدارات الحكومية، وتأكيد الأجهزة الأمنية على استخدام أدوات الشبكات وتطبيقاتها البرمجية التي تصنّع محلياً لضمان أمن المعلومات، من جهة، ونتيجة للحصار التقني المفروض على البلاد، مما جعل هذه المكونات تعاني من فقر وتقادم تقني، مما يؤدي الى تراجع كفاءة أدائها، وعدم قدرتها على توفير خدمات الكترونية داعمة لزبائن الحكومة الالكترونية (*Shahghasemi, et.,al., 2013*).

ولتجاوز عقبة تراجع مرتبة الحكومة الالكترونية في إيران، ووجود حاجة ماسة لتحقيق نتائج إيجابية في فضائها السيبراني، فقد اشتركت كل من وزارة تقنية المعلومات والاتصالات، مع مؤسسة تقنية المعلومات في إيران، وجمعية قياس مجتمع المعلومات *Measuring the Information Society of Iran*، بإعداد خارطة طريق لبرنامج الحكومة الالكترونية، عام 2014، والتي صادقت على فقراتها المجلس الأعلى لالفضاء السيبراني (*MoICT,2015*).

وتضمنت خارطة الطريق النظام الداخلي لتطوير الخدمات الالكترونية التي تقوم بها الهيئات الحكومية ـ التنفيذية، بالإضافة الى بيان طبيعة المعايير التقنية والتنظيمية لعملية تطوير هذه الخدمات. وقد وجهت خارطة الطريق عنايتها بتحديد أهداف الحكومة الالكترونية وأهدافها التنظيمية الشاملة، مع بيان كيفية إعادة هندسة متطلبات تطوير البنية التحتية لضمان بلوغ حكومة إلكترونية مميزة، وخصائص قواعد البيانات التي يستمد منها نظام الحكومة الالكترونية موارد خدماته، وهيكلة مراكز تبادل المعلومات، بالإضافة الى تحديد مهام الجهات التنفيذية، وطبيعة المهام التي ستنهض بها مؤسسة تقنية المعلومات في إيران *Information Technology Organization of Iran*.

ولا يتوقع أن تحدث تطورات سريعة في هيكلة الحكومة الالكترونية ـ الإيرانية وخدماتها، خلال المستقبل القريب، خصوصاً بعد تلاحم نسيجها الشبكاتي مع شبكة الانترنيت الوطنية *SHOMA* والتي ستحمل لها المزيد من العقبات التقنية، والتنظيمية.

5. سياسات حوكمة وتضييق قنوات فضاء الانترنيت الإيراني:

تحتل إيران رأس قائمة أشدّ الدول عداءً للانترنيت وذلك لتميزها عن بقية الدول بحظر طيف واسع من المواقع وباختلاف مضامين توجهاتها وانتماءاتها (*Faris&Villeneuve,2008*).

كما عدها البعض ثقب الانترنيت الأسود *Internet Black Hole* الذي يتبوأ المرتبة الثالثة عشر على صعيد ابتلاع وكف الكثير من خدمات الانترنيت ليحرم موانيها منها بحجة الحفاظ على القيم الأخلاقية والدينية التي جاءت بها الثورة الإسلامية للبلاد. في حين صنفت مجموعة مراسلين بلا حدود الفرنسية إيران، مع الصين، وبيلاروسيا، والسعودية كوريا الشمالية ضمنت قائمة أعداء الانترنيت *Internet Enemies* بسبب المحددات الصارمة التي يعكفون بفرضها على فضاء الانترنيت المفتوح (*Sanati,2009*).

وقد برر عضو المجلس الأعلى للمعلومات بإيران سياسة الحظر والكف السيبراني التي تمارسها الدولة على الفيض السيبراني لشبكة الانترنيت، بأنه محاولة لترسيخ قيمة المجتمع الإيراني المسلم، والتي تختلف الى حد كبير مع محتوى المواد التي يحفل بها هذا الفضاء الذي لم يلتزم بمثل هذه القيم السامية وارتبط بمنظومة القيم الغربية التي لا تتوافق مع خطاطتنا العقدية (*Sanati,2009*).

بالمقابل، أظهرت الدراسة المستفيضة التي قامت بها مؤسسة دار الحرية *Freedom House* (لتقييم مستويات الحرية التي يتمتع بها مستخدم الانترنيت في إيران خلال عام 2015) وجود أكثر من عقبة قد فرضتها الإدارة السيبرانية بالبلاد على حزمة الفيض السيبراني ومادة المحتوى المطروح على مواقع الويب لتقليص فضاء الحرية ومراقبة المستخدم الإيراني.

فعلى صعيد العقبات التي تضعها الحكومة امام عملية الوصول الى الخدمة بلغ مستوى الحرية 20 (الذي تتراوح قيمته بين 0-25) ، اما على صعيد المحددات المفروضة على المحتوى السيبراني فقد بلغ مستوى الحرية 31 (الذي تتراوح قيمته بين 0-35)، أما على صعيد التجاوز على الحقوق الشخصية للمستخدم فقد بلغ مستوى الحرية 36 (الذي تتراوح قيمته بين 0-40)، ويضاف الى ذلك حظر خدمات منصات شبكات التواصل الاجتماعي، على التوازي مع حظر طيف واسع من المحتوى السياسي والاجتماعي الذي يتعارض مع ثوابت ثقافة الثورة الإسلامية، وخطاب المرجعية الدينية، بحيث كانت الحصيلة النهائية لهذه المؤشرات[72] 100/87 (*Freedom House,2015*).

5. 1 . البيئة التشريعية الحاضنة للانترنيت:

شاع استخدام الانترنيت في منتصف عقد التسعينات من القرن العشرين، وكان الخط الهاتفي الأرضي، يمثل قناة الاتصال الوحيدة بهذا الفضاء المفتوح. وقد تزايد حجم إقبال الإيرانيين على فضاء معرفي مفتوح، ووسط سهل للتعبير عن الآراء والافصاح عنها دون وجود الحواجز الصلبة التي تحول دون ذلك على أرض الواقع المحافظ.

ومع بدايات الألفية الجديدة أضحت الحاجة الى أماكن عامة لاستقبال رواد فضاء الانترنيت حتمية، فانتشرت مقاهي الانترنيت في طهران، بكثافة، قبل أن تستنسخ هذه الفكرة في بقية محافظات البلاد كي تستقبل الزوار الذين أصيبوا بآفة الإدمان على استخدام الانترنيت وتغييب أنفسهم في فضائها بعيداً عن فضاء الواقع، ومن خلال منظومات فردية ترتبط بالأقمار الصناعية.

[72] . تؤشر القيمة الصفرية لمستويات الحرية، والحصيلة النهائية لهذه المؤشرات الى توفر حرية تامة وعدم وجود أي نمط من أنماط الحظر أو التلصص على الحقوق الشخصية للمستخدم، بينما تؤشر القيمة العليا الى غياب أي نوع من الحرية ووجود حظر كلي، وغياب الحرية الشخصية. لذا تعد إيران، وفق هذه المعايير، من الدول التي تغيب عنها جل أنماط الحريات ذات الصلة باستخدام فضاء الانترنيت، مع حجب المحتوى السيبراني لطيف واسع من المسائل ذات الصلة بالمضامين السياسية والاجتماعية، والعقدية.

ولم يغب هذا الأمر عن أنظار القائد الأعلى، الامام علي خامنئي، والذي صدر عن مكتبه في مايو من عام 2001 أمراً حمل عنوان "السياسات الشاملة حول البيانات التي تزودها شبكات المعلومات" حثّ فيه الإدارات الحكومية على حصر عملية الوصول الى المعلومات من الفضاء العولمي للانترنيت متاحاً، فقط، من خلال الكيانات السيبرانية الحكومية ـ المرخصة (*ICRTC,2005*).

كانت هذه الخطوة سابقة مهمة لتأسيس بيئة تشريعية وطنية ترعى حضور فضاء الانترنيت وتوجه مسارات استخداماته المتكاثرة. ولم تمر سوى فترة قصيرة حتى أدلى المجلس الأعلى للثورة الثقافية *Cultural Revolution High Council* (*CRHC*) دلوه في صياغة حزمة من القوانين لإدارة وتنظيم عملية الوصول الى المعلومات ومواقع الانترنيت، ما لبثت أن قدمت أمام أنظار الحكومة الايرانية.

تضمنت هذه الزمة من القوانين والتشريعات حصر جميع منافذ الوصول الى الانترنيت بالمؤسسة الحكومية حصراً، ومنعت مقاهي الانترنيت، وبقية مجهزي الخدمة من الوصول الى المنافذ العولمية، بصورة مباشرة، ووجهت بارتباطاتها بالمنفذ الحكومي ـ الحصري.

كذلك ألزمت الجهات المجهزة للخدمة بنصب وتشغيل نظم لحضر المواقع وترشيح المحتوى الذي تحفل به المواقع غير الأخلاقية، وتلك التي تناهض خطاطة الثورة الإسلامية، أو تتناول مسائل سياسية محظورة بالبلاد. ويمكن إحكام تطبيق فحوى هذه التشريعات من خلال تسجيل هوية المستخدمين، مع سجل استخداماتهم لدى مقاهي الانترنيت، والتي ستكون عرضة للتدقيق من قبل المجلس الأعلى للأمن الوطني *High Council of National Security* (*HCNS*) أو هيئة قضائية تشرف عليها وزارة تقنية المعلومات والاتصالات. وهناك محددات وقيود أخرى اقترحت ضمن لباب مادة هذه التشريعات، يصعب تناولها، إلا أنها دارت في فضاء الترشيد القسري للاستخدام وحوّلت الفضاء المفتوح الى مساحة ضيّقة تحفل بالمآزق والمطبات الأمنية والجنائية (*ICRTC,2005*).

وجاءت استجابة الحكومة في نهاية عام 2002 بعد أن أصدرت مرسوماً قضى بتشكيل هيئة تنهض بمهمة تحديد المواقع غير المرخصة لحماية الثقافة الإسلامية والارث الحضاري الإيراني من التشويه. تألفت الهيئة من ممثلين عن: وزارة المعلومات والاتصالات، ووزارة الثقافة، والإرشاد الإسلامي، وإذاعة الحكومة الإسلامية في إيران، والمجلس الأعلى للثورة الثقافية، ومؤسسة الدعوة الإسلامية. وانحصر واجب أعضاء هذه الهيئة بتحديد المعايير التي تدرج بموجبها المواقع ضمن قائمة الحظر، على أن تقدم الى وزارة تقنية المعلومات والاتصالات لتنفيذ عمليات الحظر.

من جهة أخرى، صادق البرلمان الإيراني في 17 نوفمبر 2008 على مضمون قانون جرائم الفضاء السيبراني، بينما نال موافقة مجلس الحرس *Guardian Council* بعد بضعة أيام من انقضاء زوبعة الحملة الانتخابية في 12 يونيو 2009. وقد منح هذا القانون، الحكومة الإيرانية، الحق بفرض هيمنتها على مساحة من مشهد خدمة الانترنيت بحيث تفوقت على السلطة التي تمتعت بها الدولة عند إحكام سيطرتها على مادة المطبوعات بواسطة قانون النشر، بعد أن وفرت للحكومة فرصة تحديد تخوم الممارسة المشروعة، والممارسة المحظورة مع ترسيخ قدرة الحكومة في معاقبة الذين يتجاوزون حمى الفضاء السيبراني الايراني (*ONI,2013*).

وتمتع القانون بثلاث سمات أساسية (*ONI,2013*):

- ✓ إنشاء كيان حكومي ـ مركزي يمارس مهمة مراقبة وحظر مواقع الانترنيت مع توفير بيئة تشريعية داعمة.

- ✓ ألزم مجهزي خدمة الانترنيت في عموم البلاد للتعاون مع الحكومة في عملية الحظر وترشيح المحتوى، وإدامة مراقبة الأنشطة المريبة لمستخدمي الانترنيت[73].
- ✓ تجريم عملية الدخول الى المواقع المحظورة سواء تمت عملية الدخول بصورة مباشرة، أو بواسطة أدوات التحايل السيبراني *Circumvention Tools*[74].

أحدث القانون الجديد نقلة نوعية على صعيد مناخ الحظر والتقطير السيبراني وكان بداية لتشكيل كيان مؤسسي أطلق عليه هيئة تقدير حالات المحتوى الجنائي *CDICC* وهي كيان يستمد سلطته من سلطة وزارة العدل، ويتمتع بسلطة قانونية، ويتمتع برؤية واضحة تدعمه في صناعة قرارات حاسمة على صعيد مسائل الحظر السيبراني وتقطير المحتوى السيبراني.

كذلك، ويعد تشكيل المجلس الأعلى لالفضاء السيبراني عام 2012 من الخطوات الحاسمة التي أسهمت في ترسيخ وتوطيد دعائم عمليات الحظر السيبراني وترشيح المحتوى السيبراني بعد أن أصبح هناك كيان مركزي يعنى بجميع المسائل الأساسية والتفصيلية لالفضاء السيبراني في إيران، ومن ضمنها مسألة الحظر وتقطير المحتوى.

يضاف الى ذلك وجود كيانات أخرى باتت تساهم في عمليات مراقبة محتوى الفيض السيبراني، مثل وزارة مخابرات إيران *Iran's Intelligence Ministry* وقسم تقنية المعلومات في قوى الشرطة الإيرانية *Information Communication Technology Section of Iran's Police Forces (FAVA/ICT Police)*، الذي يستمر في مراقبة محتوى مواقع الانترنيت ونمط استخداماتها بالمحفظات الإيرانية. ولم تغب هذه المسألة عن بال قيادة الحرس الثوري الإيراني، والتي أوكلت مسألة المراقبة، ومباشرة الحظر على المواقع التي تتعارض مع نهجها العسكري والسياسي، والأمني، بالإضافة الى محاربتها لجرائم المعلومات المنظمة بالبلاد (*ONI,2013*).

بالمقابل، لا يوجد لغاية هذا التاريخ تشريع قانوني ينظم ممارسات المراقبة والحظر على محتوى الرسائل القصيرة، والتي تستخدم بكثرة في الهواتف المحمولة. بيد أن المجلس الأعلى لالفضاء السيبراني *SCC* لا زال مستمراً بالتنسيق مع وزارة الثقافة والإرشاد الإسلامي (منذ عام 2013) لإعداد قانون جديد يعالج مسألة مراقبة محتوى الرسائل النصية، والتي تعد من المسائل الشائكة بسبب الحجم الهائل من مادتها التي ينتج خطابها اليومي، إضافة الى احتواء مادتها على نسيج هجين من الكلمات والعبارا ت العامية التي ليس من الهيّن ممارسة التنقير فيها، كما أن عملية حظر غير مدروسة يمكن أن تؤدي الى أزمة كبيرة بين المواطن الإيراني والحكومة (*F.H,2015*).

وفي الوقت ذاته قامت السلطة التنظيمية لاتصالات إيران *CRA* بإصدار تعليمات لتنظيم وإدارة مادة الرسائل القصيرة *SMS* والتي ألزمت جميع الجهات التجارية التي توظف هذه الخدمة بتقديم محتوى كل رسالة من هذه الرسائل الى هذه الإدارة لغرض مراجعتها قبل عملية الارسال. بيد أن المسألة ليست بهذه السهولة ولا زالت هناك الكثير من العقبات التي ستقف أمام المجلس الأعلى لالفضاء السيبراني عند معالجة هذه المسألة، بتشعباتها، ومتاهاتها التقنية والاجتماعية، الأمر الذي يؤكد استمرار غياب مثل هذا التشريع بالوقت الحالي عن ساحة الاتصالات الإيرانية.

أما على صعيد إدارة عمل مقاهي الانترنيت، فقد أصدرت شرطة الفضاء السيبراني الإيرانية، في بداية عام 2012، تعليمات حول التنظيمات التي ستلزم بها إدارات مقاهي الانترنيت في البلاد والتي تضمنت نصب كاميرات مراقبة

---

[73] . ألزم قانون جرائم الفضاء السيبراني مجهزي خدمة الانترنيت بالتقيد في جميع قرارات الهيئة مع الاحتفاظ بنسخة من بيانات المرور السيبراني لمدة لا تقل عن ستة أشهر، والتي تتضمن جميع تفاصيل أنشطة الحاسب التي يمارسها مستخدم الانترنيت، بالإضافة الى تفاصيل المعلومات الشخصية للمستخدم، وموقع التوطن الجغرافي، ورقم الهاتف المحمول.

[74] . لم تشر أي فقرة من فقرات قانون جرائم الالفضاء السيبرانيي الى استخدام الشبكات الخاصة الافتراضية *VPN* بيد أن هيئة تقدير حالات المحتوى الجنائي قد استغلت ضبابية بعض فقرات القانون لتسارع الى تجريم مستخدمي هذه الشبكات، أي أداة تستخدم للتحايل على مسارات قنوات الفيض السيبراني للانترنيت (*ONI,2013*).

أنشطة المستخدمين مع توفير سجلات تفصيلية لزوار المقهى تثبت في أسماءهم، وأرقام هواتهم المحمولة، وعنونة الحاسب المستخدم، بالإضافة الى توقيت الاستخدام، مع الاحتفاظ بسجل للمواقع التي قام بزيارتها أثناء وجوده بالمقهى. كما منعت إدارة المقهى من تنصيب برمجيات الاحتيال السيبراني، وبرمجيات الشبكات الافتراضية الخاصة *VPN* أو ترويجها بين المستخدمين (*SMO,2015,a*).

تتميز تشريعات الانترنيت في إيران بصرامتها مع ميل السلطة القضائية الى إيقاع أقصى العقوبات بمستخدمي الانترنيت الذين يخالفون فقراتها، وهناك الكثير من الوقائع التي نقلتها التقارير الدولية (*SMO,2015,b*) والتي تظهر مبالغة السلطات في معاقبة الكثير من مستخدمي الانترنيت لممارسات لا تكاد تقع بدائرة المخالفة لدى دول أخرى، نذكر منها: الحكم على ثمانية من المستخدمين الشباب بالسجن لمدة تراكمية قدرها 127 عاماً بسبب نشرهم مواد مناهضة للحكومة على صفحات موقع *Facebook*، والحكم بالسجن لمدة 11 عاماً على مدوّن نشر مدونة نقد فيها النظام الإيراني، وغيرها الكثير من الوقائع التي تؤكد صرامة الإجراءات التي تتخذ ضد أي مخالفة أو نشر رأي تراه مؤسسات النظام مناهضاً للثورة الإسلامية وثقافتها.

5 . 2 . البيئة المؤسسية المشرفة على أمن فضاء الانترنيت:

تتألف معمارية المؤسسات الإيرانية التي تحدد سياسة الحظر والحجب السيبراني من مجموعة طبقات تشكّل البنية الهرمية التي تتكون مما يلي:

الطبقة الأولى: يستقر فيها، وعلى قمة هذه الهيكلة الهرمية، القائد الأعلى للثورة الإسلامية، آية الله علي خامنئي. ويتمتع القائد الأعلى بصلاحيات حصرية واسعة تشمل: تحديد الإطار التشريعي ومحددات سياسة اتصالات الانترنيت في البلاد، وتسمية القيادات العسكرية، والأمنية، والحكومية التي تساهم في المؤسسات والهيئات التي تمارس عملية حظر وترشيح محتوى المواقع.

الطبقة الثانية: المجلس الأعلى لالفضاء السيبراني *SCC*، الذي يعد السلطة العليا لصياغة سياسات ومحددات استخدام الانترنيت، ومختلف النشاطات التي تمارس في الفضاء السيبراني السيبراني، وعلى الصعيدين الوطني، والعولمي.

الطبقة الثالثة: هيئة تقدير حالات المحتوى الجنائي *CDICC* والذي يعد المسؤول المباشر عن تحديد مادة المحتوى السيبراني الذي ينبغي ترشيحه، والمواقع وصفحات الويب التي ينبغي حظرها. كما تقوم الهيئة بتحديث قوائم تضم أسماء وعناوين المواقع التي تضم صفحاتها محتوى يخالف خطاطة ثقافة الثورة الإسلامية وقاعدتها الأخلاقية، وتلك التي تهدد الأمن الوطني، أو تتناول بالنقد مؤسسات الدولة، أو قيادات الدولة.

وتتقاسم هذه الهيئة مع المجلس الأعلى لالفضاء السيبراني سبعة من الأعضاء، الأمر الذي يؤكد وجود فجوة، على مستوى المسؤوليات والصلاحيات بين صنّاع السياسات السيبرانية، وتطبيق قرارات الحظر والحجب السيبراني.

الطبقة الرابعة: وتتألف من المؤسسات الحكومية التنفيذية، والتي تترأسها وزارة تقنية المعلومات والاتصالات الإيرانية *MoICT* والتي تنهض بمهام: تنفيذ الحظر على المواقع المدرجة في قوائم هيئة تقدير حالات المحتوى الجنائي، وتشغيل شبكة الانترنيت الوطنية *SHOMA*، بالإضافة الى إدارة البنية التحتية للانترنيت ومنظومات الاتصال كافة في البلاد. وتلتحق بهذه الطبقة شركة البنية التحتية للاتصالات *TIC*، والتي تعد الجهة الحصرية لتزويد حزمة الانترنيت في البلاد.

الطبقة الخامسة: جهات تنفيذية تنتمي الى المؤسسة العسكرية أو الأمنية، منها الجيش الإيراني السيبراني *Iranian Cyber Army ICA* وهي مؤسسة مختلطة تتألف من قوات نظامية ومجموعة من المتطوعين من قراصنة المعلومات

والمدوّنين الذي يناصرون الثورة الإسلامية وينافحون عن منجزاتها في الفضاء السيبراني، فيقومون بمراقبة الأنشطة المريبة على الشبكة ويقومون بهجمات مضادة لأي تعرض يحصل في فضاء الانترنيت بإيران.

وتشترك بالتوطن في هذه الطبقة، شرطة الفضاء السيبراني *FATA* التي تمارس دور محاربة جرائم المعلومات، ومتابعة موارد التهديدات السيبرانية ضد كيانات شبكة المعلومات الإيرانية، والمستخدمين. وبالوقت ذاته، تلعب مؤسسة الحرس الثوري ـ الإيراني دوراً جوهرياً، ضمن هذه الهيكلة الهرمية، ومن خلال جناحها الاستخباري، الذي يقوم بإدارة عمليات مختلفة في الفضاء السيبراني للدفاع عن حمى البلاد، وبالتنسيق المباشر مع الجيش الإيراني السيبراني.

5 . 3 . حظر المواقع وتقطير مادة المحتوى السيبراني:

بدأت عملية مراقبة وحظر مواقع الويب أثناء ولاية خاتمي، عام 2005، واتسمت بنهج غابت عنه سمة التعقيد، مع اعتماد قواعد بسيطة استرشدت بها عملية الحظر شملت المواقع المنافية للأخلاق، وأخرى تعارض صراحة وتنادي بمعاداة الثورة الإسلامية وثقافتها في إيران.

وقد مرّت عملية الحظر بطفرة نوعية بعيد الحملة الانتخابية لعام 2009، بعد أن تأججت المواجهة بين المعارضة وأنصار الرئيس محمود أحمدي نجاد، ولاستخدام المكثف لتطبيقات منصة شبكات التواصل الاجتماعي، مع تناسل المدوّنات السيبرانية، والنمو المطّرد للمحتوى السيبراني المطروح في فضائها، بحيث استشعرت القيادات الإيرانية بحجم المخاطر التي يمكن أن تنشأ عن فضاء الانترنيت وتطبيقاته التي حشّدت معارض النظام والثورة بشكل غير مسبوق.

لم تسترشد عملية الحظر السيبراني وكف المواقع، في بداياتها، بتوصيات جهة تقع على عاتقها مسؤولية تشخيص هوية وعنونة المواقع التي يراد حظرها، كما لم يكن لدى إدارة الرئيس خاتمي خطط واضحة للتعامل مع هذه المسألة. فاتسمت العملية بمعالجات آنية، وتوصيات من جهات تستوطن في المنظومات العقدية، أو الأمنية، أو السياسية، أو مراجعات قامت بها الكوادر التي تعمل في وزارة تقنية المعلومات والاتصالات.

ومع تعاظم اهتمام السلطة بهذه المسألة، وتزايد تأثيراتها المباشرة وغير المباشرة على الكثير من الملفات الداخلية، والتي صاحبتها ظاهرة تكاثر الهيئات والمجالس التي تعنى بملف المعلومات والاتصالات في البلاد خلال السنوات 2005-2009، وصدور قانون جرائم الفضاء السيبراني الذي ولدت، نتيجة لما ورد في مضمون إحدى فقراته، هيئة تحديد المحتوى الجنائي للمواقع الالكترونية *CDICC* التي كانت لادتها في بدايات عام 2009.

وأضحت هذه الهيئة الجهة الوحيدة التي تمتلك تخويلاً قانونياً لممارسة عملية صياغة معايير حظر المواقع المخالفة، وتحديد هويتها، وبيان مبررات عملية الحظر. وتقوم الهيئة بتحديث قواعد بيانات الحظر وتعميمها على الجهات المعنية، بصورة مستمرة لضمان إحكام السيطرة على استخدامات فضاء الانترنيت في إيران (*ONI,2009*).

وتقع مهمة تنفيذ عملية حظر المواقع التي تستوطن قوائم الهيئة، على عاتق قسم الحظر السيبراني في شركة إيران لتقنية المعلومات *ITC*، احدى تشكيلات وزارة تقنية المعلومات والاتصالات. أما شركة البنية التحتية للاتصالات *Communication Infrastructure Company* (*CIC*) فقد أوكلت إليها مهمة توحيد مهمة إجراءات الحظر في عموم البلاد.

مرّت عملية الحظر السيبراني في إيران بمراحل متعددة، حيث تظهر الحفريات في تربتها وجود تراتبية متصاعدة باتجاه تضييق الخناق على تدفق الفيض السيبراني في قنوات فضائها السيبراني سنة، بعد سنة، نتيجة للضغوط التي تمارسها المؤسسات العقدية، والأمنية، والتشريعية للتقليل من مخاوفها وهواجسها المتزايدة من آثار حرب غير معلنة تسافر تهديداتها في النبضات السيبرانية التي تتدفق في قنوات فيض الانترنيت وفضائها المعقد.

بداية يتألف فضاء الحظر السيبراني في إيران من أربع طبقات، خططت الإدارة الحكومية، والمؤسسات المسؤولة عن إدارة الفضاء السيبراني أن يتكامل أداءها الى مستوى يضمن إحكام إدارة الفضاء السيبراني بالبلاد بحيث يتوافق مع ثقافة الثورة، ويدرئ بالوقت ذاته، الأخطار المحتملة من تسلل أعداء البلاد من خلال الثغرات السيبرانية، أو إساءة استخدامه لممارسة سلوك عدواني أو جنائي على خصوصية المستخدمين أو مواردهم السيبرانية، أو المادية.

بصورة عامة، تمارس في فضاء الطبقة الأولى سلسلة من عمليات المعالجة السيبرانية لسد الثغرات، وتعهد خلو فضاء الانترنيت من موارد ومواقع معلوماتية تتعارض مع خطاطة الثورة الإسلامية وثقافتها. أما الطبقة الثانية فتشمل مجموع التشريعات التي تحاول تنظيم وإدارة استخدام فضاء الانترنيت من خلال ضوابط وعقوبات زاجرة تحدّ من الإبحار غير الملتزم بالفضاء السيبراني المفتوح. في حين يستهدف من إرساء الطبقة الثالثة حضور كيانات ومؤسسات أمنية تقوم بعملية المراقبة والمتابعة، لسلوك المستخدمين للكشف عن التجاوزات، وكفّها، أو التقليل من آثارها المحتملة، وتحديد هوية المتجاوزين وتسليمهم الى العدالة لينالوا عقابهم وفق الأطر التشريعية السائدة بالبلاد.

وتعد الطبقة الرابعة الحل الجذري الذي تروم الحكومة الإيرانية بلوغه حيث سيتم تحويل جميع أنشطة فضاء مجتمعها السيبراني باتجاه فضاء شبكة الانترنيت الوطنية *SHOMA* التي ستعمل بمعزل عن فضاء الانترنيت العولمي، وسيتشكل من خلال نسيجها الشبكاتي نسيج وطني بصبغة إيرانية صرفه، وبلسان فارسي مبين، وإدارة مطلقة للحكومة الإيرانية على جميع مفردات ترابطاته الشبكاتية وعناصر محتواه السيبراني.

بوشر بحظر مواقع الانترنيت، عام 2005، عند نهاية ولاية الرئيس الإيراني محمد خاتمي، وبدأت إجراءاتها تتصاعد شيئاً فشيئاً بعد الأحداث التي عصفت بالشارع الإيراني أثناء الحملة الانتخابية عام 2009، وبعد أن ترسخت القناعة لدى طبقة المحافظين ومؤسسة الحرس الثوري الإيراني بحجم التهديدات التي يمكن أن تزاول عن طريق تطبيقات شبكات التواصل الاجتماعي، ويمكن أن ينشب عنها تهديدات على مستوى الاستقرار الأمني بالبلاد، وما تحمله من تهديدات محتملة لمكتسبات الثورة الإسلامية وثقافتها.

جاءت الدعوات لممارسة الحظر متأخرة، وبعد أن تغلغلت خدمة الانترنيت وأشربت قلوب المواطن الإيراني بما يوفره فضاءها المفتوح من انفتاح عولمي، ويعمق التواصل مع الآخر ضمن تطبيقات شبكات التواصل الاجتماعي. وثبت تناقض الدعوات المتشنجة التي صدع بها البعض للبدء فوراً بقطع خدمة الانترنيت، ومنع تمدد فضاءها المشحون بالمحظورات والتهديدات التي باتت تسافر بحرية في فضاء الثورة الإسلامية، فلم يعد أمام مؤسسات الثورة الإسلامية، بجميع مفاصلها، سوى القبول بممارسة عملية حظر ممنهجة على المواقع التي تتناقض مضامينها مع أهداف الثورة وغاياتها، وتلك التي تحوي مادة محظورة تتنافى مع الأخلاق والقيم الإسلامية.

وشأن جميع عمليات حظر مواقع الانترنيت المتكاثرة، لم تحقق المعالجات السيبرانية نتائجاً مشجعة نتيجة للتناسل المستمر في أعداد المواقع المحظورة، والتي يصعب حصرها، ووجود أدوات متنوعة للاحتيال السيبراني، تتوفر بالمجان على مواقع الانترنيت، مع وجود رغبة مزروعة في النفس الإنسانية للولوج في مجالات المحظور لإشباع غريزة الفضول الملتصقة بالنفس الإنسانية.

وبعد أن باشرت السلطات الإيرانية بتبني آلية حظر المواقع وممارسة عمليات تقطير المحتوى السيبراني للمواقع توجهت الإدارة الأمريكية الى التعاقد مع إحدى الشركات العملاقة بمضمار أمن المعلومات للعمل على كسر الشيفرات السيبرانية المستخدمة في عمليات الحظر، مع تخصيص مفوّض رقمي *Proxy* ـ مجاني (*ziaiy.persianblog.com*)، أتاح للمستخدمين الإيرانيين فرصة تجاوز عقبة الحظر المفروض على فضاء الانترنيت، مع الالتزام بحظر المواقع غير الأخلاقية التي تتنافى مع ميول عامة الشعب الإيراني (*Anoosheh,2012*).

وبعد مدة يسيرة صادق الكونغرس الأمريكي في عام 2007، على مشروع أكثر اتساعاً وشمولاً لممارسات الحكومات المناهضة للانترنيت، والتي تتبنى سياسات حظر المواقع، وتقطير المحتوى خصصت له ميزانية ضخمة بلغت 50 مليار دولار لدعم الشعوب على تجاوز عقبة الحظر المفروض على فضاء الانترنيت، والتنقل بحرية في فضائه الرحيب. وقد باشر المشروع بتسخير تقنيات المعلومات والاتصالات لتوفير حلول ناجعة تدعم المستخدمين في الدول المعادية للانترنيت بوسائل وآليات متنوعة وفّرت لهم بالمجان للتسلل عبر قنوات اتصال آمنة لبلوغ فضاء معلومات يتجاوز المحددات التي تفرضها الدول على فضاء الانترنيت.

أطلق على الفضاء الجديد الذي اصطنعته الشركات العاملة تحت مظلة المشروع الأمريكي اصطلاح "الانترنيت في حقيبة السفر *Internet in Suitcase*" أو "ظل الانترنيت *Internet Shadow*". عد هذا المشروع نزعة جديدة للإدارة الأمريكية في توجيه مسارات استخدام الانترنيت في دول الشرق الأوسط، وبضمنها إيران الخصم العنيد. ولم تمضي سوى مدة قصيرة حتى أعلن موقف الحكومة الإيرانية من المشروع الجديد على لسان الناطق بلسان ووزارة الخارجية الإيرانية، رامين مهمان باراست، والذي عد هذا المشروع خطوة مناهضة لحقوق الانسان، وأن الجيش السيبراني الإيراني لن يقف مكتوفاً قبالة هذا النوع من المشاريع التي تناهض المسار الذي اختطته الثورة الإسلامية بإيران، وسيبذل ما في وسعه لإفشال أهداف هذا المشروع العدواني.

5 . 3 . 1 . إحكام السيطرة على منافذ الاتصال بفضاء الانترنيت:

تعد بوابة قنوات الاتصال بفضاء الانترنيت، من المسائل الحيوية التي تمنح أجهزة المراقبة فرصة إحكام سيطرتها، وترسيخ سلطتها على المادة المسافرة في فضاء قنواتها السيبرانية المختلفة.

وقد فرضت الإدارة الحكومية في إيران، هيمنتها المطلقة على قطاع المعلومات والاتصالات، بعد أن أوكلت لوزارة المعلومات والاتصالات *MICT* هذه المسؤولية وربطت بهيكلها التنظيمي عملية إدارة جميع أنشطة شركة البنية التحتية للاتصالات *TIC* التي استأثرت بإدارة سوق الاتصالات والمعلومات في البلاد[75]، وتفردت بسيطرتها على منفذ تزويد وتحديد سعة خدمة الانترنيت المجهزة للقطاعين الحكومي والخاص بإيران من خلال امتلاكها لشركة إيران لاتصالات البيانات *DCI* والتي تعد المجهز الأساسي للخدمة *Main ISP*.

بصورة عامة ترتبط جميع قنوات فضاء الانترنيت الحكومي ببوابة شركة *TCI*، أما شركات تجهيز الخدمة للقطاع الخاص فإن بواباتها تنصاع أيضاً للارتباط بالمنفذ الوحيد المقيم لدى الشركة ذاتها. وبذلك أصبحت الإدارة الحكومية قادرة على فرض سياسة الحظر والحجب من نقطة الشروع التي تقيم لدى الشركة المذكورة، كما تمتلك جميع مادة الفيض السيبراني على صعيد صفحات ويب المواقع، والبريد الالكتروني، والرسائل السريعة، دون أن تتوفر فرصة لتسللها بعيداً عن عينها المراقبة بعناية، وإحكام بواسطة خوادم التفويض التي تقوم بهذه المهمة.

وتشترك مع هذه مؤسسة أخرى هي معهد البحوث في العلوم الأساسية *Institute for Research in Fundamental Sciences IRFS* والتي تقوم بمهمة تسجيل أسماء النطاق *Domain Names* التي تحمل العنوان *".ir"*. لذا فإن عملية الترخيص لجميع الجهات المرتبطة بمجهزي الخدمة الملتحقة بالقطاع الخاص الإيراني، تدار دفتها لتلتحق أسماء أنطقتها بالجهة الحكومية (*ONI,2013*).

---

75 . رغم النداءات المتكررة منذ عام 2007 لخصخصة شركة البنية التحتية للاتصالات، فقد تحركت مؤسسة الحرس الثوري الإيراني الى تسمية شركة *Mobin Trust Consortium* والتي استحوذت على 50 % من الحصة السوقية لشركة *TCI* فضمنت ارتباطها بها، وبقيت هذه الشركة مملوكة للحكومة الإيرانية، وأقصي القطاع الخاص عن الاستثمار فيها.

5 . 3 . 2 . حظر مواقع الويب ومنصات التطبيقات:

تنفرد إيران، عن بقية الدول المعادية للانترنيت، التي تعتمد نظم حظر مواقع الانترنيت، في تبنيها سياسة مشددة بالتعامل مع المحتوى السيبراني وذلك من خلال ممارستها عملية الحظر على مواقع الويب التي تحتوي صفحاتها على كلمة من الكلمات المفتاحية التي أدرجت لديها في لائحة الكلمات والعبارات المحظورة، في حين تحظر بقية الدول صفحات الويب التي تحتوي عنونتها على الكلمات المفتاحية (مثل الصين، والسعودية، واليمن ودول أخرى) .(*Faris*& *Villeneuve*,*2008*)

ويمكن أن تؤرخ بدايات استخدام آلية الحظر السيبراني في إيران، بالتوجيه الذي صدر عن مكتب القائد الأعلى للثورة، علي خامنئي، عام 2002، ودعا فيه الى ضرورة وجود سياسة واضحة لتحديد مسارات وضوابط الأنشطة التي تمارس في فضاء شبكات المعلومات بعموم البلاد (*Aryan, et.al.,2013*).

في البداية، ارتكزت عملية حظر مواقع الانترنيت في إيران الى معمارية (مبسطة) قوامها طبقتين[76] وسادها ثلاثة أساليب لاستكمال دائرة هذه العملية. امتدت الطبقة الأولى على جميع نقاط الوصول الى خدمة الانترنيت *Access Service Points* (*ASP*) والتي تهيمن على نسيجها الشبكاتي شركة اتصالات إيران. واستخدم الشركة برمجيات الحظر الشهيرة *SmartFilter* (ذات المنشأ الأمريكي) في ضبط عنونة وهوية المواقع التي يسمح للمواطن الإيراني بالوصول إليها، وتلك التي يحظر عليه الدخول إليها. أما الطبقة الثانية فشملت جميع مجهزي خدمة الانترنيت *ISP's* ومجهزي خدمة الانترنيت التجارية *Internet Commercial Providers* (*ICP's*) (الذين تصلهم قنوات الخدمة من شركة اتصالات إيران) على استخدام برمجيات حظر إضافية لتضييق الخناق على قنوات الخدمة، والالتزام بتحديث قوائم المواقع المحظورة، والتي تزودهم بها الجهات الحكومية، وبصورة دائميه.

أما الأساليب فقد تميزت باستخدام تقنيات مبسطة (قبل سنة 2004) شملت: إلزام الشركات المجهزة للخدمة بالبلاد بإغلاق المنافذ التي يحاول المستخدمون من خلالها تجاوز عقبة الحظر، مع الحرص على الكشف عن هوية خوادم التفويض التي تدعم عمليات الاحتيال السيبراني لغرض إدراجها في قوائم حظر المنافذ السيبرانية. أما الأسلوب الثاني فقد استخدمت فيه الكلمات المفتاحية *Keywords* التي توحي الى المواضيع والمسائل المحظورة، التي استقرّت في عنونة مواقع الويب *URL*. وقد أوكلت هذه المهمة الى مجهزي خدمة الانترنيت لمنع المستخدمين من الوصول الى هذه المواقع من خلال استخدام برمجيات حظر تعتمد هذه الآلية في عملها.

أما الأسلوب الثالث فتشرف عليه وزارة تقنية المعلومات والاتصالات من خلال تضييق سرعة منافذ تجهيز الخدمة للمساكن والأماكن العامة لمنع المستخدمين من الوصول الى مواقع الملفات المرئية، ومواقع تحتاج الى سرعة كبيرة لضمان غياب قدرة التواصل لدى المستخدم الإيراني مع مادة المحتوى السيبراني المطروح فيها[77].

ولم تقتصر عملية الحظر والمراقبة على مواقع خصوم الثورة ومعارضيها فحسب، بل تمتد أذرعها ومجسّاتها الى مواقع رموز وقيادات إيرانية لتمارس عليها الخطاطة الأمنية ذاتها. ولعل من الشواهد على ذلك حجب موقع جمران

[76] . وقد ذهب البعض الى تبرير استخدام هذه المعمارية لغايتين: الأولى التقليل من الزخم السيبراني الذي تتحمل أعباؤه الطبقة الأولى (الحكومية) نتيجة للأعداد المتزايدة من المواقع المحظورة والتي بدأت آثارها واضحة على سرعة الانترنيت في عموم البلاد. أما الثاني هي مشاركة الجهات المجهزة لخدمة الانترنيت (القطاع الخاص) للقطاع الحكومي في مسؤولية الحفاظ على الفضاء السيبراني من إساءة الاستخدام.

[77] . أصدرت السلطة التنظيمية للاتصالات بإيران *CRA* تعليمات للشركات المجهزة لخدمة الانترنيت، حددت بموجبها سرعة حزمة الانترنيت بالقطاع السكني بحيث لا تتجاوز 128 Kbps (*Aryan, et.al.,2013*).

Jamaran الذي يقوم بتغطية أخبار عائلة القائد الأعلى ومؤسس الثورة الإسلامية في إيران، الامام الخميني، بسبب نشره لصورة الرئيس السابق محمد خاتمي، والذي حظر نشر أي أمر يتعلق به في وسائل الاعلام في المدة الأخيرة. وقد أعيد الموقع الى العمل بعد قيام إدارته برفع هذه الصورة من صفحات الموقع (*SMO,2015,a*).

ويتعرض المرور السيبراني لفضاء في أجهزة الهاتف المحمول للمحددات ذاتها التي تنشأ عن نظم المراقبة المستديمة التي تمارس على الخطوط الهاتفية الأرضية. ويستمر الحظر على المستخدم الإيراني في ممارسة التواصل المرئي (عبر خدمات الفيديو السيبراني) بالهواتف المحمولة لتكاثر النداءات التحذيرية التي أطلقتها المرجعيات والتي خشيت أن تكون هذه الممارسة سبباً مباشراً لحصول كارثة ثقافية وعقدية في إيران (*SMO,2015,b*).

وتنسق وزارة المعلومات والاتصالات مع الشركات المشغلة للهواتف المحمولة في تشغيل نظم برمجية تنقّر في محتوى الرسائل القصيرة *SMS* فتحظر منها ما احتوى الى كلمات وعبارات قد أدرجتها الجهات المعنية في قائمة المنع كونها تنافي الأخلاق أو تناهض سياسة الحكومة. وقد نقل التقرير الذي أعدته مؤسسة دار الحرية *Freedom House* قيام شركة *IranCell* بحظر الرسائل القصيرة التي احتوت على عبارة "دعنا نأكل" لأنها تستخدم شعبياً للإشارة الى أمور غير أخلاقية، كما حظرت الكثير من الرسائل القصيرة التي حوت كلمة *Mashaei* أثناء الحملة الانتخابية لعام 2009، كونها تحتمل إمكانية ارتباطها بمرشح الرئاسة، آنذاك، اسفانديار رحيم مشائي! (*F.H,2015*).

وقد تولّد عن تشدد نهج الحكومة الإيرانية في حظر مواقع الانترنيت، تزايد توجّه المستخدمين الإيرانيين نحو استخدام أدوات الاحتيال السيبراني لتجاوز الحواجز الأمنية الصارمة التي تفرضها الجدران النارية المقيمة في خوادم الانترنيت في الشركات والمؤسسات السيبرانية المرتبطة بوزارة تقنية المعلومات والاتصالات الايرانية.

من أجل هذا يلاحظ شيوع استخدام تطبيقات الشبكات الافتراضية *VPN* بين المستخدمين الإيرانيين بسبب مميزاتها الفريدة في تجاوز الحظر السيبراني. وقد أظهرت نتائج الاستبيان الذي طرحته المؤسسة البريطانية *Small Media Organization* في النصف الأول من عام 2014 حول أكثر الشبكات الافتراضية الخاصة استخداماً في البيئة الشبكاتية الإيرانية، أن الايرانيين يصنفون شبكة *TOR/ORBOT* في المرتبة الأولى، وشبكة *Browsec* بالمرتبة الثانية، وشبكة *Psiphon* في المرتبة الثالثة، وشبكة *Hotspotshield* بالمرتبة الرابعة، بينما احتلت لديهم شبكة *FreedomeVPN* المرتبة الخامسة، والتي تعد بأجمعها بوابة داعمة للمستخدم الإيراني في تجاوز عقبة الحظر وبلوغ تخوم الفضاء المفتوح للانترنيت بعيداً عن الرقابة الصارمة التي تفرضها إيران على مستخدمي الانترنيت (*SMO,2014,c*).

وبالوقت ذاته برزت محاولات جادة لمتخصصين بمضمار تقنية المعلومات، من داخل إيران وخارجها، لتوفير دعم واسناد للمستخدمين الإيرانيين بالحصول على هذه الأدوات، وتجاوز عمليات الحظر المتكررة على المواقع التي تروّج نشر هذه الأدوات. نذكر منها مشروع *FilterShekhanha* (والذي يعني مصدّعي مفتاح الحظر) الذي ولد على يد باحث الانترنيت ناريمان غريب في فبراير من عام 2014، والذي يديم عملية إرسال صحيفة أخبار الى عناوين البريد للمشتركين بهذه الخدمة بمعلومات محدثة حول أدوات التحايل على نظم الحظر المهيمنة على شبكة الانترنيت في إيران. وقد أودع عنونة صحيفته على شكل قائمة بريدية في حسابه على *Twitter* الأمر الذي يحول دون حظرها بواسطة نظم الحظر المحلية (*SMO,2015,b*).

وقد ذاع صيت هذه الصحيفة الإخبارية فبلغ عدد المشتركين بالعدد الأول منها 11,546 مشترك، ثم تناسل حضورها لدى مستخدمي الانترنيت في إيران فتجاوز عدد المشتركين بها أكثر من 100 ألف مشترك. وتحفل هذه الصحيفة بآخر أخبار أدوات التحايل الجديدة، والتحديثات الخاصة بالإصدارات الحالية، اودعها ناريمان غريب في خادم يدعم المستخدمين الإيرانيين في تنزيل تطبيقات التحايل بصورة مباشرة، وتنصيبها في الحواسب أو الهواتف الذكية لتجاوز

عقبة الحظر واستخدام منصات التواصل الاجتماعي، وغيرها من التطبيقات التي تسعى الحكومة الى حظرها عن المستخدم الإيراني.

أولاً. مصادر أدوات الحظر والمراقبة السيبرانية:

في بدايات عمليات الحظر السيبراني، استخدمت إيران برامجاً تجارية، أمريكية المنشأ، لممارسة عملية حظر المواقع ومراقبة المحتوى السيبراني (برنامج *Smart Filter*) سواء كان محتوى الموقع باللغة الإنجليزية أو اللغة الفارسية، كما وأكدت مؤسسة مبادرات الشبكة المفتوحة في إحدى تقاريرها التي سخرتها لدراسة تفاصيل عمليات الحظر السيبراني التي تمارس في إيران على فضاء الانترنيت، أن هناك أكثر من شركة أوربية قد قامت بتجهيزها ببرمجيات قادرة على مراقبة تفاصيل أنشطة المستخدمين الإيرانيين أثناء حضورهم في فضاء الانترنيت[78] (*ONI,2005*).

وللتخلص من القلق المصاحب لاستخدام أدوات وتطبيقات أجنبية (في ممارسة عملية الحظر السيبراني) داخل حدود الفضاء السيبراني الإيراني، فقد شجعت الإدارة الحكومية الجهات الأكاديمية، ومراكز البحوث والتطوير، والقطاع الخاص على البدء بدراسة وتنفيذ مشاريع تكثّف اهتمامها بإنتاج أدوات وتصميم برمجيات وطنية تقوم بهذه المهمة[79] (*ONI,2009*).

وتشير الكثير من التقارير الدولية (*ONI,2005,2009&2013*) الى تخصيص الحكومة الإيرانية لميزانية ضخمة لتمويل مجموعة من المشاريع الوطنية التي تعنى بتتبع أنشطة مواطنيها أثناء ابحارهم في فضاء الانترنيت. وتعد عملية تحويل مسار الفيض السيبراني للانترنيت من خلال خوادم التفويض *Proxy Servers* إحدى الضمانات لمراقبة وإعداد سجلات دقيقة للمواقع التي يزورها المستخدم، ولأنشطته التي تتضمن التواصل مع الغير عبر خدمة البريد الالكتروني، والرسائل القصيرة، والتعليقات التي ينشرها على مواقع شبكات التواصل الاجتماعي، الأمر الذي يدعم هذه المشاريع من خلال توفير قنوات محدودة لممارسة أنشطة التتبع والمراقبة والحظر السيبراني[80].

وتسهم معمارية منافذ خدمة الانترنيت التي توجه جميع مسارات الخدمة التي توفرها شركات تجهيز الخدمة *ISP's* من خلال نقطة وصول مركزية تستقر في رحم إحدى شركات وزارة تقنية المعلومات والاتصالات (شركة البنية التحتية لاتصالات إيران *TCI*) في توفير مناخ مناسب لعمل نظام المراقبة والحظر المركزي الذي سخرته الوزارة لتلبية الغايات السياسية والأمنية لأجهزة الدولة المختلفة.

وقد بدأت بشائر حضور صناعة إيرانية نجحت في إنتاج برمجيات وعتاد حاسوبي لمراقبة نزعات مستخدمي الانترنيت، وتقطير المحتوى السيبراني لصفحات الويب ومواقع شبكات التواصل الاجتماعي.

يستخدم الإيرانيون (بالوقت الراهن) برمجيات محلية أعدت خصيصاً لممارسة عمليات حظر المواقع من خلال نظام مركزي لديه القدرة على حجب أي موقع خلال بضع ساعات في عموم شبكات المعلومات المحلية. وتأتي هذه القدرة

---

78 . أفصحت إحدى التقارير الحكومية أن إيران قد اقتنت هذا النظام البرمجي من شركة *Nokia Siemens Networks* في عام 2008 لتوفير مناخ آمن لاستخدام الانترنيت في البلاد وحظر المواقع التي تنافي المنظومة العقدية والأخلاقية للثورة الإسلامية في إيران (*ONI,2005*).

79 . اعتبرت الإدارة الإيرانية مسألة الاعتماد على برمجيات أجنبية في عمليات مراقبة وحظر مواقع الانترنيت مؤشراً على ضعف منظومتها السيبرانية، كما أن برامج الحظر يمكن أن تستخدم من أجهزة المخابرات الأجنبية للتغلغل في شبكة المعلومات الوطنية، والتلصص على قواعد البيانات الحكومية، إضافة الى إمكانية إفصاح هذه الشركات عن طبيعة الإجراءات التي تمارسها الحكومة ضد المواقع والمستخدمين.

80 . في تصريح لقائد شرطة الالفضاء السيبرانيي *FATA* ذكر هادي أنفر لشبكة نسيم الإيرانية *Nasim Online* (في 12 سبتمبر 2014) أن مؤسسته أصبحت تمتلك الأدوات السيبرانية اللازمة لمراقبة محتوى جميع الرسائل التي يتداولها المستخدمون من خلال التطبيقات: *Viber, Tango & Whats App* كما أن لدى مؤسسته أدلة كافية يمكن تقديمها للمجلس الأعلى لالفضاء السيبراني تؤكد على ضرورة حظر جميع تطبيقات التواصل المستخدمة في الهواتف الذكية كونها تشكّل تهديداً أمنياً للبلاد (*SM,2014*). بيد أن إقرار عملية الحظر مرتهنة بقناعة هيئة تقدير حالات المحتوى الجنائي *CDICC* وهي الجهة التي تتحمل مسؤولية تنفيذ هذا الاجراء حصراً دون غيرها.

المميزة من إلزام الحكومة لجميع مجهزي خدمة الانترنيت بتوجيه مسارات قنواتهم الاتصالية (التي تحتوي على طلب الوصول الى موقع من المواقع التي يروم المستخدم الدخول اليها) الى صناديق المعالجة السيبرانية التي تمتلكها خوادم الحكومة، والتي تقوم بالتنقير عن وجود الكلمات المفتاحية ـ المحظورة، سواء في عنونة صفحة الويب، أو محتواها، وتقوم مباشرة بحظر هذه المواقع (*F.H,2015*).

إن الدعوات المتتالية الى اعتماد تقنية الحظر الذكي *Intelligent Filtering* من خلال معالجات التفحص العميق لحزم بيانات الانترنيت *Deep-Packet Inspection* (*DPI*) لبلوغ الصفحات التي تحوي المضامين الممنوعة، دون غيرها، وكثرة التصاريح التي انبثقت عن مسؤولين حكوميين حول نجاح خبراء المعلومات الإيرانيين بإنشاء نظام برمجي وطني يمارس هذه المهمة[81]، تؤكد استمرار النظام الإيراني بعملية الحظر، والسعي المستمر الى تعميق جذور عملية التنقير في المحتوى السيبراني لحجز جميع عناصر الخطاب المناهض للثورة الإسلامية، والاستمرار بمعاداة فضاء الانترنيت، ومحاربة سمة الانفتاح المقيمة في مادة نسيجه السيبراني[82].

وقد بدأت آلة برامج المراقبة والحظر تتطور في إيران خلال السنوات الأخيرة، وباشرت مراكز البحث والمؤسسات الأكاديمية بالعمل المشترك لتحقيق برنامج متكامل للمراقبة والحظر، على التوازي مع عملية التحوّل من أسلوب المعالجة التقليدية الى أسلوب المعالجة الذكية التي ستسهم بتقليص الزمن المطلوب لتحليل مادة المحتوى السيبراني، مع تجاوز عقبة توسع دائرة الحظر الذي كان لصيقاً بالمعالجات التقليدية، واقتصار الحظر على محتوى صفحات بذاتها، بدلاً من حظر الموقع برمته على المستخدمين الإيرانيين.

وبعد أن ترسخت قدم التقنية الإيرانية في مجال إنتاج برمجيات مراقبة نزعات المستخدمين، وحظر المواقع، وتقطير مادة المحتوى السيبراني، سواء كانت هذه المادة نصوصاً أو مواد مرئية، التحقت إيران بحظيرة الدول المعادية للانترنيت، والتي تتمتع بقدرات وطنية قادرة على توفير مستوى من الكفاية الأمنية لفضائها السيبراني، مثل الصين وكوريا الشمالية.

ثانياً: المواقع التي يطالها الحظر:

منذ عام 2009 شكّلت لجنة مشتركة من المجلس الأعلى للثورة الثقافية والسلطة القضائية بالبلاد لمراجعة تفاصيل وآليات حظر المواقع وكف أنشطتها من الفضاء السيبراني الإيراني.

وتدّعي وزارة المعلومات والاتصالات الإيرانية أن إيران يمكن أن تعد من أكثر الدول التي تمنح مواطنيها فرصة استخدام فضاء الانترنيت بحرية ودون فرض قيود على عملية ابحارهم بين مواقع الانترنيت كما أنها قد أتاحت للمعلومات أن تتدفق في فضائها السيبراني. واستندت الوزارة في تبريرها الى التمييز بين المواقع التي تزود المستخدم بالمعلومات، والتي تركت مفتوحة امام المواطن الإيراني ينهل منها ما يشاء دون قيود أو حظر. وبين مواقع تنشر وتروّج لممارسات تتنافى مع الخطاطة العقدية والأخلاقية للثورة، أو يستخدمها البعض للإساءة الى الرموز الدينية او الوطنية، وهي المواقع التي تمارس الوزارة عليها عمليات الحظر والكفّ وفق نهج مدروس بعناية.

---

[81] . أعلن وزير الاتصالات الإيراني في شهر شباط من عام 2015 أن المرحلة الثانية من نظام المراقبة والحظر الذي قد ابتدأت في 28 من شهر يونيو المنصرم بعد انتهاء المرحلة الأولى من المشروع بنجاح، وأن هذه المرحلة ستستمر لمدة ثلاثة أشهر قادمة. وذكر أن المشروع سيكتمل مع انتهاء مرحلته الثالثة دون أن يفصح عن التاريخ المتوقع لانتهائها (*SMO,2015,a*)

[82] . رغم أن عملية معالجة محتوى الملفات الصورية والفيديوية تعد معقدة وشبه مستحيلة في بعض الأحيان، فقد حرصت الحكومة على مباشرة سلسلة من المحاولات، والتي ذكر وزير المعلومات والاتصالات الإيراني، في إحدى تصريحاته الأخيرة، أن نظام الحظر الذكي الوطني قد أصبح قادراً على تحليل محتوى مواقع الفيديو (مثل You Tube)، ومواقع الصور (مثل Instagramوغيره من المواقع) وحظر المادة التي تحتوي على مادة صورية منافية للأخلاق أو مناهضة للنظام (*F.H,2015*).

وعلى صعيد متصل ذكر المدير العام لشبكة تقنية المعلومات، إسماعيل رادكاني، بأنه قد تم تشكيل هيئتين لغرض حظر مواقع الفئة الثانية، وبواقع 1000 موقع جديد شهرياً، بالإضافة الى المواقع التي تحظر بصورة آلية نتيجة لترويجها المسائل الإباحية، ومضيفات التفويض *Proxy Server* التي تدعم وصول المستخدمين الى المواقع المحظورة. وقد قدّر عدد المواقع المحظورة في سنة 2009 بحوالي مليون موقع، تحوي حوالي 90 % مواداً إباحية وأخرى منافية للأخلاق (*Sanati,2009*).

بيد أن الملاحظ أن عملية الحظر والكفّ لم تشمل هذه المواقع فحسب، بل شملت كثير من المواقع السياسية، والاجتماعية، ومواقع تيارات دينية غير محافظة، ومواقع الدفاع عن حقوق الانسان، ومواقع دعم حقوق المرأة، وتيارات سياسية محلية، وجمعيات إصلاحية لا تتوافق خطاباتها مع الخطاب السياسي والعقدي لقيادات الثورة الإسلامية المهيمنة على دفة الحكم بالبلاد ـ أنظر الجدول (3 -25).

الجدول (3 - 25) ـ أنواع المواقع وطبيعة المحتوى المحظور في الفضاء السيبراني الإيراني.

الموقع أو المحتوى	سياسة وإجراءات الحظر
مواقع الويب[83].	يصار الى حظر مواقع الويب في ضوء قوائم الحظر التي تعدها هيئة تحديد المواقع غير المرخصة (والتي تحدث بصورة شهرية)، ومن خلال حظر أسماء نطاقاتها *Domain Names*. وتلتحق بالمواقع المحظورة: ☒ مواقع الدعارة والتي تحظر بصورة كلية (100%). ☒ المواقع الجنسية ومواقع الثقافة الجنسية بمختلف توجهاتها. ☒ مواقع حقوق الانسان ومنظمات المجتمع المدني. ☒ مواقع الأديان غير الإسلامية، أو الفرق الإسلامية المناهضة للتشيع. ☒ المواقع السياسية وبمختلف توجهاتها، (داخل إيران وخارجها) وبنسب تصل الى 98 %. ☒ مواقع الحركات النسوية والدعوة الى حقوق المرأة. ☒ مواقع الأخبار التي لا تدين بالولاء لخطاطة الثورة الإسلامية وثقافتها. ☒ مواقع ناقدة للحكومة الإيرانية وأخرى تتهكم برموزها العقدية والسياسية. ☒ مواقع برمجيات مكافحة عمليات الحظر والبرمجيات محظورة الاستخدام.
المدوّنات السيبرانية.	لا يمكن حصر مواضيع المدونات التي تتعرض لعملية الحظر بسبب كثرة المواضيع التي تناقشها، وتنوّع مضامينها. وتكاد تسري عليها خطاطة حظر مواقع الويب، ويضاف اليها المدونات الشخصية التي يفصح أصحابها عن آرائهم بصدد ما يحصل على أرض الواقع، بمختلف تفاصيلها.
محركات البحث.	حظر موقع البحث الشهير *Google* وخدماته السيبرانية المختلفة ومن ضمنها خدمة البريد الالكتروني *GMAIL* منذ عام 2013. وتبذل الإدارات السيبرانية الإيرانية جهوداً حديثة لنشر استخدام محركات البحث الوطنية لجذب المستخدم الإيراني بعيداً عن محركات البحث العولمية.

[83] . يضاف اليها، كذلك، المواقع التي تعالج مواضيع: التحول السياسي والأحزاب المعارضة، الإصلاح السياسي والتشريعي، المسلحين والمتطرفين والإرهابيين، حقوق الأقليات، خطاب الكراهية، المواعدة، القمار والرهان، الكحول والمخدرات، القرصنة السيبرانية، الاستضافة المجانية للمواقع، خدمات البريد الالكتروني المجانية، الترجمة، المشاركة بوسائط البيانات، وشبكات التواصل الاجتماعي.

الموقع أو المحتوى	سياسة وإجراءات الحظر
منصات شبكات التواصل الاجتماعي.	حظرت مواقع التواصل الاجتماعي مثل: *Facebook, Twitter, You Tube &Instagram* عن المستخدمين الإيرانيين رغم استخدامها من قبل قيادات سياسية، مثل القائد الأعلى ، ورئيس الجمهورية، ووزير الخارجية.
خدمات التراسل والتواصل عبر الهاتف الأرضي والمحمول.	تتوفر لدى الإدارة الحكومية الإيرانية الأدوات الكافية لمراقبة جميع اتصالات الهواتف الأرضية والمحمولة، كما أنها تقوم بحظر تطبيقات الهواتف الذكية التي يمكن للمستخدم أن يبث من خلالها خطاباً معارضا للنظام فقد حظرت خدمة منصة تطبيق *Viber* بعد إغلاق خدمة *WeChat* كما أن زوبعة حظر تطبيق *WhatsApp* لا تخفى عمن يتابع مسائل هذه الملف المتشعبة (*SMO,2014,a*).
مواقع أدوات الاحتيال السيبراني.	تحظر مواقع نشر أدوات الاحتيال السيبراني وتوضيح كيفية استخدامها وذلك لإقبال المستخدمين الإيرانيين على توظيفها لتجاوز عقبة الحظر السيبراني.
خوادم التفويض.	تمارس الجدران السيبرانية الإيرانية مهمة حظر خوادم التفويض التي تدعم ارتباط المستخدمين الإيرانيين بالعالم الخارجي (*Sennhauser,2009*).

ثالثاً: الخطاطة التي تعتمدها الحكومة في عمليات الحظر:

بصورة عامة، يمكن تلخيص الخطاطة التي تتبناها الإدارة الحكومية في إيران في مراقبة، وتتبع أنشطة المستخدمين، وحظر المواقع وتقطير المحتوى السيبراني بنهج يتألف من ثلاثة أنماط من المعالجات. والتي تشمل معالجات وقائية *Preventive*، وأخرى تعرّضية *Interceptive*، وثالثة تفاعلية *Reactive* (*Robertson&Marchant,2014*).

ويتضمن النوع الأول من المعالجات استخدام حزمة متنوعة من الأدوات وبرمجيات الكفّ السيبراني التي تسعى الى منع المستخدم الإيراني من الدخول الى المواقع، ومطالعة صفحات الويب المحظورة دون أن تحاول التعرّف على هوية هذا المستخدم، أو مراقبة أنماط حضوره في فضاء الانترنيت.

أما النوع الثاني فيتضمن مباشرة سلسلة من الإجراءات (غير المعلنة) والتي تحاول الكشف عن هوية المستخدم، وأنماط حضوره في فضاء الانترنيت، مع السعي لمراجعة مادة خطابه السيبراني، وتحديد الموقع الذي ينطلق منه نشاطه ، بعد أن أضحى نطاق نشاطه قريباً من الحمى السيبراني الوطني، وبات يستقر على قائمة الجهات المناهضة للنظام وثقافته.

ويأتي النوع الثالث لكي يستكمل تجميع البيانات والمعلومات التي تدعم الإجراءات الأمنية التي تحكم عملية مراقبة جميع أنشطته، وتتبع قنوات تحركاته واتصالاته ضمن فضاء الانترنيت لاعتراض ما قد ينجم عنها من تأثيرات مباشرة، أو أخرى مباشرة، وللانقضاض عليه متى استكملت الوقائع التي تثبت ممارسته الجرمية بحسب فحوى فقرات قانون جرائم الفضاء السيبراني.

وفي الوقت ذاته تلجأ أدارات أمن المعلومات الى استخدام أسلوب القرصنة بوصفها أداة ناجعة لاستهداف الناشطين الإيرانيين وخصوم الحكومة المقيمين في فضاء الانترنيت. تضمنت الدراسة المستفيضة التي قامت بها مجموعة أمن المعلومات *FireEye* قيام مجموعة من القراصنة الإيرانيين، أطلقت على نفسها، *Ajax Security Team* بعملية قرصنة واسعة النطاق (أطلقت عليها اسم *Operation Saffron Rose*) استهدفت مواقع ويب وهجمات حجب خدمة، بالإضافة الى نصب شراك رقمية *Digital Decoy* للإيقاع بمستخدمي الانترنيت المحليين ممن يرومون الحصول على أدوات الاحتيال السيبراني، والتي تمنحهم فرصة القفز فوق نظم الحجب السيبراني المستخدم في البلاد.

وقد حاولنا استقصاء الآليات التي اعتمدتها الإدارة الحكومية في إيران لممارسة عملية الحظر على مواقع الويب وتقطير مادة المحتوى السيبراني خلال العقد الأخير ـ أنظر الجدول (3 - 26).

الجدول (3 - 26) ـ الآليات السيبرانية التي تستخدم لتنفيذ خطاطة المراقبة والتتبع والحظر في الفضاء السيبراني الإيراني.

نهج المعالجة	الآليات السيبرانية المستخدمة
معالجات وقائية.	● إعادة توجيه مسارات أسماء النطاقات والقائمة السوداء للمواقع والتي تعد من التقنيات المتقادمة والتي اعتمدتها الإدارة السيبرانية بإيران والتي حظرت بواسطتها نطاق المواقع المحظورة مع تحويل مسار الفيض نحو شركة اتصالات إيران *TIC*. ● استخدام برمجيات التحكم بمحتوى صفحات الويب *Content Control Software* والتي تنظم عملية الاتصال بالخوادم ومراجعة الكلمات المفتاحية المحظورة. ● تضييق سرعة خدمة الانترنيت على المستخدم (بحيث لا تتجاوز 128 Kbps) لضمان عدم وصوله الى مواقع التواصل الفيديوي وغيرها من المواقع التي تتطلب وجود حزمة عريضة.
معالجات تعرضية.	● الفحص المتعمق لحزم المعلومات *Deep Packet Inspection* والتي تعد من المعالجات الذكية لمحتوى صفحات مواقع الويب وتقطيرها والتي تستخدم لإدامة مراقبة محتوى الفيض السيبراني لمواقع الانترنيت، وحظر المواقع المحظورة، وتقطير مادة المحتوى المناهض للنظام ومؤسساته المختلفة. ● تقنية رجل في الوسط *Man-in-the-Middle* (*MITM*) والتي تستخدم لمقاطعة الاتصالات السيبرانية الآنية وسبر مادة محتواها. ● تحليل المرور السيبراني Traffic Analysis وذلك باستخدام برمجيات ذكية قادرة على سبر مادة الخطاب السيبراني والكشف عن المادة المحظورة المستودعة في عباراته.
معالجات تفاعلية.	● تتبع الأنماط المحظورة التي تتواجد في مادة التواصل السيبراني للمستخدم، أو في عنونة المواقع التي يكثر الدخول اليها أثناء حضوره في الفضاء السيبراني ومقارنتها مع قواعد بيانات توظف المتغير المعرفي لتشخيص حالات الوصول الى المناطق المحظورة. ● تتبع ممارسات الناشطين السيبرانيين في فضاء الانترنيت والتنسيق مع شرطة فضاء الانترنيت *FATA* لتحديد مواقعهم والقبض عليهم. ● الحظر الدوري لبروتوكول طبقة منافذ الأمن *SSL* والتي تستخدم لاجتياز عقبة الحظر من خلال برمجيات التواصل بين الخوادم والمستخدمين. ● التضييق الآني قنوات الفيض السيبراني لفضاء الانترنيت في ضوء معطيات الواقع لضمان كفّ عمليات وصول المستخدم الإيراني الى فضاء التطبيقات المحظورة، أو تلك التي تستخدم لمناهضة مفاصل النظام المختلفة.

المصدر: (*Robertson&Marchant,2014*).

ويظهر بجلاء من بيانات الجدول أن الإدارة السيبرانية لم تترك باباً إلا وطرقته في بحثها الدؤوب عن أفضل آلية تضمن إحكام السيطرة على قنوات فضاء الانترنيت، مواقعاً ومحتوى، بيد أن سمة الانفتاح التي يتسم بها هذا الفضاء، ووفرة أدوات الاحتيال السيبراني، وكثرة مواقع القرصنة السيبرانية التي توفر الدعم للمستخدمين لا زالت تشكّل تحدياً كبيراً لهذه المعالجات.

5 . 3 . 3 . نظام الحظر والترشيح الذكي:

أكثر المسؤولون الإيرانيين من استخدام اصطلاح الحظر الذكي منذ بداية عام 2014 في الإشارة الى السعي الحثيث للإدارة الحكومية في حظر المواقع وتقطير المحتوى المسافر مع حزمة رقمية تتجاوز سعتها 1,200 Gb بدلاً من حظر نطاق الخدمة بأجمعه، وللتقليل من حجم النفقات المطلوبة لعملية الحظر السائدة في فضاء الانترنيت بإيران (*SMO,2014,c*).

وقد عكفت أكثر من مؤسسة بحثية وأكاديمية على إعداد برنامج الحظر الذكي الذي لا يقتصر على تتبع الكلمات المفتاحية الموجودة في عنونة مواقع الويب، وإنما يستمر في التنقير عن حضور هذه الكلمات داخل محتوى صفحات الويب لغرض انتخاب الصفحات المرشحة للحظر بدلاً من حظر الموقع بأكمله.

وقد استخدمت الإدارة السيبرانية لمشروع نظام الحظر والترشيح الذكي برنامجين، ينتمي كل منهما الى حقل من حقول المعالجة المحوسبة الذكية. ويعمل هذين البرنامجين، على التوازي (بقصد ضمان بلوغ كفاءة عالية في المعالجة الآنية) لممارسة عمليات المعالجة الذكية التي تقوم بحظر المحتوى المحظور في صفحات منتخبة من المواقع، عن طريق مزاولة عملية التقطير السيبراني للمادة المحظورة في مرحلتين تكمل إحداهما عمل الأخرى (*Majlesi,2015*).

وتحدث وكيل وزير تقنية المعلومات والاتصالات عن وجود مرحلة معالجة سابقة للنظام الذكي والتي ستحدد هوية جميع مستخدمي الانترنيت، بصورة آلية بتوظيف قواعد بيانات ترتكز الى معالجات معرفية متقدمة قامت بإعدادها شركات وطنية تعتمد نظم ترتكز بكثافة الى الموارد المعرفية *Knowledge- Based Resources* لضمان حظر الجزء المحظور من مواقع شبكات التواصل الاجتماعي مع استبقاء بقية المحتوى دون حظر (*Majlesi,2015*).

من جهة أخرى ورد بالتقرير الذي أعدته جريدة *Azer News* حول نظام الحظر والترشيح الذكي فقد نقلت عن وزير تقنية المعلومات والاتصالات الإيراني، أن هذا النظام سوف يكون قادراً على ترشيح المحتوى السيبراني لفضاء الانترنيت على صعيد النصوص، والصور، ومقاطع الفيديو، وبكفاءة عالية (*Niayesh,2015*).

وعلى صعيد متصل تحدث علي كاظمي (أحد الخبراء الإيرانيين الذين يعملون على نظام الترشيح الذكي للانترنيت *Intelligent Filtering*) عن بعض الميزات المهمة التي سيتمتع بها هذا النظام (*SM,2014*):

- ✓ سيكون النظام قادراً على تمييز عنوان صفحة الويب *URL* ويستطيع حجب جزء محدد من العنونة الفرعية للصفحة، فيحجب صفحة محددة من الموقع، أو فقرة من فقرات صفحة موقع *Facebook*.
- ✓ سيقوم النظام بتحديد مستويات مختلفة للوصول لكل مستخدم من المستخدمين. وستوفر هوية المستخدم، وموقعه في قائمة المستخدمين (موظف/طالب/أستاذ جامعي،...) بحيث يمكنه الوصول الى المواقع التي تتوافق مع توجهاته، وقد تتعارض مع توجهات مستخدم آخر.
- ✓ سيوفر النظام أدوات قادرة على تحليل محتوى الملفات المرئية *Videos*، والصور، والملفات الصوتية، وتمارس دور الحظر متى أثمرت عملية التحليل عن العثور على محتوى محظور. بيد أن عملية الحظر لا تشمل جميع محتويات صفحة الموقع بل تنال الفقرة المخالفة بينما تبقى بقية الكائنات السيبرانية صالحة للاستخدام.

إن القراءة المتأنية لبعض الخصائص التي أباح بها هذا الخبير، تؤكد وجود مبالغة متعمدة في الإعلان عنها لتوليد قلق ومخاوف متزايدة لدى المواطن الإيراني من الاستخدام غير الملتزم بخطاطة الثورة الإسلامية، فيعرض عن استعراض مثل هذه المواقع. أما من الناحية التقنية فإن مثل هذا النظام سيؤدي لا محالة الى حصول تباطؤ ملحوظ في عملية تصفح المواقع، لأن عملية تحليل الملفات المرئية، والصوتية، وغيرها من الملفات، تتميز بوجود تعقيد في بنيتها

البرمجية، الأمر الذي سيؤدي الى بطء كبير في عملية الاستعراض، بالإضافة الى حظر الكثير من الملفات، غير المحظورة، نتيجة عدم قدرة خوارزمية النظام على التمييز الدقيق بين تفاصيل المحتوى المحظور عن المحتوى السليم[84].

ولم تمر سوى بضعة أيام على تصريح هذا الخبير حتى أعلن المركز الوطني لالفضاء السيبراني *National Center of Cyberspace NCC*، في 29 سبتمبر 2014، عن إطلاق الاصدارة الأولى لنظام الحجب والترشيح الذكي، والذي يمتلك القدرة على حجب وحظر المواقع التي تضم محتوى ينافي الأخلاق العامة (سواء كان مادة مرئية، أو صورية، أو نصوص). وقد استخدم هذا التطبيق البرمجي، للمرة الأولى، في مركز بحوث جامعة الشهيد بهشتي (*SM,2014*).

ورغم الهالة التي أنشأتها الإدارة السيبرانية الإيرانية حول نظام الحظر والترشيح الذكي الذي ولد عن بذرة إيرانية ولدت في تربة فضائها السيبراني، فإن هناك الكثير من الشكوك التي تحوم حوله، والتي تؤكد أن مثل هذه المعالجة لن تمارس دورها بشكل سليم في عملية الحظر، كما أن عملها سيؤدي الى خلخلة أداء الفضاء السيبراني وتباطؤه بشكل غير مسبوق (*Advocacy,2015*).

ونكاد نتلمس تأكيدات عما ذهبنا إليه من التقرير الذي عكفت على إعداده مجموعة البحث ضمن حملة حقوق الانسان بإيران (والتي تتبعت أنماط الحظر التي تمارسها الإدارات السيبرانية ـ الايرانية على المحتوى السيبراني) والذي نفت (من خلاله) صحة ادعاءات هذه الجهات باستخدام نظام ترشيح ذكي قادر على تمييز جميع أشكال المواد المحظورة في صفحات الويب[85]، وعدته دعاية إعلامية، ومحاولة لإخافة المستخدم الإيراني من الدخول الى المواقع التي تتعارض مع خطاب الثورة الإسلامية (*ICHR,2015*).

وأكّدت بالوقت ذاته على وجود سعي حثيث على اقتراح أساليب أكثر نجاعة في ضمان تنفيذ خطاطة المجلس الأعلى لالفضاء السيبراني في بلوغ مستوى عال من عمليات حظر المحتوى المناهض للثورة وتوجهاتها السياسية والعقدية. حيث اقترحت بعض الجهات المتخصصة بأمن المعلومات غض النظر عن مشروع الحظر الذكي والتوجه نحو آلية جديدة، تتوجه نحو المستخدم الإيراني، بدلاً من توجهها نحو الفيض السيبراني الهادر، حيث اقترح منح كل مستخدم هوية رقمية تحتفظ الحكومة بتوثيق جميع معلوماته الشخصية، وتستخدم سجل رقمي لتتبع جميع تحركاته، ومسارات البحث التي يمارسها أثناء وجوده في فضاء الانترنيت، وتودعها ضمن قواعد البيانات كي تسهل عملية تحليلها وممارسة الحظر الذي يتوافق مع طبيعة تحصيله العلمي، أو انتمائه الاجتماعي، وفئته العمرية، وغيرها من العوامل الملتصقة بهويته فتوفر له نطاقاً للتنقل في مجال فضاء يتباين الى حد كبير مع بقية فضاءات المجاميع الأخرى (*ICHR,2015*).

إن المتخصصين بحقول أمن المعلومات على دراية تامة عن غياب أي فرصة لبلوغ حظر مثالي يلتزم بمعايير محددة دون أن يمس بكفاءة وسرعة شبكة المعلومات، أو يتجاوز على مساحة قد لا تقطع ضمن نطاق الحظر فيحرم شريحة من المستخدمين من بيانات مهمة، لذا فإن تمسك التيار المتشدد في الإدارة الحكومية، والتشريعية، والعقدية، ومبالغة مؤسسة الحرس الثوري الإيراني في مطالباتها بترشيح طيف واسع من مادة المحتوى وإدراجها ضمن قطاع الأمن القومي للبلاد سيؤدي بالنهاية الى التوجه نحو قطع الوصلة التي تصل المستخدم بالفضاء السيبراني العولمي، وربطه بفضاء

---

84 . ذكر علي بهشتي، الأستاذ في جامعة شريف للتقنية، أن نظام الحظر والترشيح الذكي لن يستكمل جميع أدواته في وقت قريب، كما أن فرصة حظر النصوص في تطبيقات التواصل الاجتماعي ستكون ممكنة، أما على صعيد الملفات المرئية والصورية، والصوتية فإنها إن نجحت فستؤدي الى حصول تباطؤ شديد في خدمة الانترنيت (*SM,2014*).

85 . بررت المجموعة عدم قدرة الإدارة السيبرانية في إيران على ممارسة هذا النوع من الحظر الذي بسبب استخدام معظم هذه المواقع نظام شهادات تشفير *SSL*، والتي لا تسمح بعملية سبر المحتوى والتنقير في مادته عن عناصر محددة، يضاف الى ذلك أن حجم المرور السيبراني في إيران قد توسّع بحيث لا يمكن أن تتوفر إمكانية لنظام قادر على المعالجة الآنية للكم الهائل من مواد المحتوى بمختلف أشكالها.

شبكة الانترنيت الوطنية *SHOMA* والتي لن تتخلص إدارتها من مطالب جديدة لممارسة الحظر على محتوى مواقع الشبكة الوطنية، والمحتوى التواصلي الذي سيبثه المستخدمون الإيرانيون أثناء حضورهم في شبكات التواصل الاجتماعي، أو فضاء المدونات.

5 . 3 . 4 . التحوّل النهائي نحو فضاء *SHOMA* المتوحّد:

تعد عملية إنشاء شبكة المعلومات الوطنية *SHOMA* خطوة مهمة نحو إعادة توجيه مسارات فيض الفضاء السيبراني وتنفيذ سياسة الحظر السيبراني بإقصاء المستخدم الإيراني عن الفضاء العولمي، وابقائه داخل حدود فضاء محلي مورست عملية تشكيل مادة محتواه السيبراني بحيث تتطابق بالكلية مع أهداف الثورة الإسلامية ونهجها السياسي، والعقدي، والثقافي.

وبهذا النهج سوف تتقلص مهام المراقبة من فضاء عولمي مفتوح، يحفل بمواقع معادية يصعب حصرها، ومحتوى رقمي لا تتوفر فرصة لاحتوائه، ومعالجته لضمان خلوه من أي خطاب معارض، الى فضاء محلي، تدار مواقعه من خلال عملية الترخيص الحكومي لأصحاب المواقع الملتزمين حصراً بقواعد اللعبة التي فرضتها، بينما سيراقب المحتوى المطروح فيه وفي فضاء تطبيقات شبكات التواصل الاجتماعي ـ المحلية، وفضاء المدونات ومواقع المنتديات الإيرانية بسهولة ويسر، لقوقعها جميعاً في قبضة إدارة تمسك بجميع تلابيبه، ولا يكاد يخرج عن دائرة عينها المراقبة أي صغيرة أو كبيرة تضاف الى مادة المحتوى السيبراني لمواقعه، أو تسافر في قنوات التواصل بين مستخدميه.

5 . 4 . الحظر السيبراني وتنازع السلطات:

لا يمكن الإمساك بتلابيب مسألة صناعة القرار لدى الإدارات الإيرانية التي تعنى بحوكمة الفضاء السيبراني ما لم نمارس نهجاً تبسيطياً لحلحلة تشابك خيوط تنازع مراكز القوى وتجاذبها في بلاد تهيمن عليها مجموعة واسعة من المؤسسات التي تدين بالولاء للمنظومات العقدية، والأمنية، والسياسية، بحيث يصعب تمييز خارطة الطريق الذي تسلكه قراراتها.

بيد أن وجود القائد الأعلى للثورة الإسلامية، وطبيعة السلطات الواسعة التي قد منحت له، يسهم في ممارسة دور توفيقي يخفف من وطأة التناقض، وحدة التجاذب بين الإدارة المعتدلة لحسن روحاني، والمنظومة الحوزوية، والحرس الثوري الإيراني، والمتشددين في مجلس الشورى الذين يبالغون في تضييق الخناق على الفضاء السيبراني بالبلاد، ويحرمون مواطنيهم من سمة الانفتاح التي يتمتع بها هذا الفضاء العولمي.

ولما كان فضاء الدولة مثقلاً بهيمنة خطاطة ثقافة الثورة الإسلامية، بحيث لا تكاد تعثر على رقعة صغيرة لم توظف فيها الخطاطة العقدية التي تتعامل مع جميع مفاصل الحياة بوصفها جزءاً لا يتجزأ من عقيدة الثورة وممارساتها، لذا ما انفكت عملية بلوغ سياسة ثابتة تجاه التعامل مع الفضاء السيبراني بعيدة المنال، كما أن تبني سياسة اصطناع مجالس عليا، وهيئات لحل إشكالية الصراع المحتدم بين المتشددين، والمعتدلين ستستمر ولأمد بعيد، بسبب صرامة المؤسسات العقدية والحرس الثوري من جهة، وعناد المعتدلين وعدم رضوخهم للسلطة القاهرة التي يمتلكها المتشددون، من جهة أخرى.

وقد بات جلياً لدينا، ومن خلال متابعة قراءاتنا لهيكلة مؤسسات حوكمة الفضاء السيبراني والاتصالات في إيران، كثرة الولادات لمؤسسات تبزغ براعمها، داخل حدود حمى هذه الجهة أو تلك، وبلوغها مرحلة الشيخوخة قبل أن تينع أغصانها، لتستبدل بأخرى، والنتيجة هي المزيد من تشتت القرارات، وتحميل الموازنة الحكومية حجماً هائلاً من التخصيصات المالية لتلبية مطالب جهات بعيدة عن تقنية المعلومات والاتصالات، وإنهاك الطبقة العارفة والخبيرة

(من المتخصصين بتقنيات المعلومات والاتصالات وحوسبة المحتوى) بأعباء إضافية لتحقيق غايات قد يصعب، أو يستحيل نوالها.

ولم تخل ساحة حظر المواقع وحجب المحتوى من سمة تنازع السلطات، وتكاثر الآراء، ومحاولة القفز على صلاحيات الهيئات التي أنيطت بها مسؤولية ممارسة هذه المهمة. فتنطلق دعوات من أعضاء المجلس الإيراني، وأخرى من المؤسسة الحوزوية، وثالثة من المؤسسة التشريعية[86]، بالإضافة الى ما تعلن عنه المؤسسات الأمنية، والحرس الثوري الإيراني.

أما ما يتعلق بالأمن القومي للبلاد، والمسائل التي لا يعلن بها على أسماع الملأ فهي أكثر بكثير، الأمر الذي سبّب ولا يزال يسبب ارباكاً شديداً لدى المؤسسة التقنية، ولدى الهيئات السيبرانية عند صناعة قرارتها التي يمكن أن تعقد موقفها قبالة المنظومات العقدية، والعسكرية، والأمنية.

كذلك قد بادرت بعض المؤسسات الى ممارسة عملية الحظر عبر إجراءات تقع خارج دائرة الحظر السيبراني، بنوعيه الذكي، أو التقليدي من خلال عدم إصدار التراخيص[87]، أو قيام مؤسسة شرطة الالفضاء السيبرانيي بإجراءاتها دون مراجعة الجهات المعنية[88].

بالمقابل، لا يستشعر الحرس الثوري الإيراني أي حرج في ممارسة الكثير من مهام مراقبة محتوى المواقع، وممارسة عملية الحظر، أو إلقاء القبض على المخالفين، متجاوزاً حدود بقية المؤسسات المعنية، ودون أن تفكر قياداته بمخاطبة هذه الجهات أو الاستئناس برأيها حول كل حالة من هذه الحالات.

وتزدحم التقارير والدراسات التي تقوم بها المؤسسات الدولية التي تعنى بسياسات الحظر المعلومات في إيران (*SMO,2013,b*)، والمنظمات التي تعنى بحقوق الانسان (*F.H,2015*) بإيراد شواهد كثيرة تؤكد استئثار هذه المؤسسة بكثير من الإجراءات التي تقفز من فوق الصلاحيات التي تتمتع بها جهات أمنية وأخرى تقنية تعنى بمثل هذه المسائل.

ولعل من الشواهد على هذا السلوك المتسلط التصريح الذي صدع به الخبير في الفضاء السيبراني بالحرس الثوري، علي زاده، أثناء اللقاء الذي أجرته معه القناة الأولى بوكالة الإذاعة بالدولة *IRIB 1*في فاتحة شهر شباط عام 2015 والذي تحدّث فيه صراحة عن قيام مؤسسته بجملة من هذه الإجراءات، نذكر منها (*SMO,2015,a*):

- ☒ قيام مؤسسة الحرس الثوري بمراقبة شاملة لجميع شبكات التواصل الاجتماعي، وأن من يعتقد من المستخدمين الإيرانيين أنه بمأمن من العقاب حال ممارسته أنشطة محظورة فإنه واهم.
- ☒ قامت مؤسسة الحرس الثوري بإلغاء 130 صفحة من تطبيق التواصل الاجتماعي *Facebook* مع القاء القبض على 12 من أصحاب هذه الصفحات لإساءة استخدامها.

---

[86] . أرسل النائب العام في إيران، غلام حسين محسني الايجي، الى وزير تقنية المعلومات والاتصالات في 20 سبتمبر 2014 مطالباً إياه في حظر خدمة مواقع *Viber, Tango & Whats App* خلال مدة أقصاها شهر. وقد برر طلبه بتداول سلسلة من المازحات حول الامام الخميني بين المستخدمين الإيرانيين منذ بداية هذا الشهر. من جهته ذهب عبد السلام أمد خرم آبادي (سكرتير *CDICC*) أن عجز وزير تقنية المعلومات والاتصالات عن المباشرة بعملية على هذه التطبيقات سيدفع هيئته الى حظر عمل هذه المنصة التواصلية لأن المحتوى المطروح فيها بات يشكل تهديداً للأمن القومي. ولم يتأخر رد وزير تقنية المعلومات والاتصالات على طلب النائب العام، وتعليقات سكرتير هيئة *CDICC* بأنه رغم حرص وزارته على حظر المحتوى المحظور، إلا انها تعتقد بأن حظر تطبيق ما، أو منصة شبكة تواصل اجتماعي لا يعد إجراءً سليماً، لوجود أكثر من مجال توظف فيه هذه التطبيقات يدعم تواصل المستخدمين الإيرانيين بعيداً عما ذكر في طلب النائب العام (*SM,2014*).

[87] . أغلقت المواقع الإخبارية المحافظة *Dana.ir* وحظر وصول المستخدمين الإيرانيين اليها لفشلها بالحصول على رخصة من وزارة الثقافة والإرشاد الإسلامي *Ministry of Culture and Islamic Guidance (MCIG)* وقد رفع الحظر بعد حصول التصريح في 4 سبتمبر 2014 (*SM,2014*).

[88] . قامت شرطة الالفضاء السيبرانيي بإلقاء القبض على مجموعة أساءت استخدام مواقع شبكات التواصل الاجتماعي خلال الربع الأخير من عام 2014.

☒ تشخيص أكثر من 350 صفحة على موقع *Facebook* تحوي صفحاتها على مادة تدعو الى إحداث تغيير في نمط الحياة بإيران، يخالف ثقافة الثورة الإسلامية.

5 . 4 . 1 . تراتبية صناعة وتنفيذ قرارات الحظر السيبراني:

تتوطن التجاذبات التي تستهدف إدارة سياسة حظر مواقع الانترنيت في إيران، على مساحة واسعة وتتشتت مقاعد أصحاب القرار فيها بين أكثر من جهة، وتتعدد ولاءاتها، وتتباين مستويات السلطة التي تتمتع بها، مع تداخل مجالات مسؤولياتها، بينما تشترك جميعاً بعدم وضوح الرؤية حول كيفية تنفيذ القرارات التي قد تصدر، في كثير من الأحيان، عن جهات لا تستطيع تحديد حجم العمل المطلوب لتنفيذ قراراتها، وهل أن هذه القرارات تقع ضمن دائرة الممكن، ، أم أنها تستقر بعيداً في دائرة المستحيل إزاء القدرات التي تسخرها التقنيات السيبرانية المتاحة (سواء على الصعيد المحلي أم العولمي).

ويضاف الى ذلك وجود تناقض صريح بين تصريحات الجهات التي تمارس صناعة جزء من نسيج هذه القرارات، والتي تصدع بالدعوة الى قطيعة مستديمة[89]، أو الى انفتاح جزئي، أو تنادي بسياسة تتألف مادتها من مجموعة قرارات تتناوب السماح والحظر وفق قواعد لا تبدو رشيدة في كثير من الأحيان، وإنما تؤشر الى قرارات آنية تصطنع نتيجة لتصارع مراكز القوى وتنافسها على الإمساك بتلابيب السلطة في البلاد.

بصورة عامة، تتألف معمارية صناعة القرارات الخاصة بملف الحظر السيبراني (داخل المؤسسة الحكومية الإيرانية) من هيكلة هرمية تتنقل فيما بينها الأنشطة والإجراءات التي تتخذ لحماية بيئة الفضاء السيبراني الإيراني، وضمان توافقها مع سياسة الحكومة وثقافة الثورة الإيرانية.

وقد بدأت سمة التعقيد في الهيكلة المؤسسية التي بدأت تتناسل منذ عام 2009، مع تنازع السلطة على إدارة الفضاء السيبراني، بجانبيه التخطيطي، والتنفيذي، بين عدة جهات تستقر بعضها ضمن المؤسسة الحكومية، وأخرى في المؤسسة العقدية، وجهات ذات صلة بالملف العسكري والأمني. فنجم عن ذلك تعقد نسيج مسارات صناعة القرارات، وتداخل الصلاحيات، وعدم توازن توزيع المسؤوليات بين جهات متعددة، وتحمل ولاءات متباينة (*Aryan, et.al.,2013*).

رغم استقرار القائد الأعلى للثورة الإسلامية على قمة هرم جميع مفاصل الملف السيبراني، إلا انه لا يمارس نشاطاً مباشراً على صعيد عملية الحظر باستثناء نتائج ترجمة توجيهاته في لقاءاته المتكررة، والتي يسترشد بها صناع القرار في المجلس الأعلى لالفضاء السيبراني *SCC* في تحديد النهج الذي يتوافق مع توجيهاته وترجمتها الى إجراءات لصيقة بموضوع مراقبة وحظر المواقع في فضاء الانترنيت.

وتأتي في المرتبة الثانية السياسات والقرارات التي يتخذها المجلس الأعلى لالفضاء السيبراني بخصوص هذه المسألة، وتشعباتها المختلفة. وتكاد أن تشترك هيئة تحديد حالات المحتوى الجنائي *CDICC* المرتبة ذاتها للمجلس الأعلى لالفضاء السيبراني بعد أن منحها قانون جرائم الفضاء السيبراني الإيراني سلطة مطلقة في تحديد هوية مواقع الويب وطبيعة المحتوى الذي يجب حظره عن مستخدمي الانترنيت في إيران. وقد حددت الهيئة الإطار العام لقرارات الحظر والتي ترتبط باحتواء المواقع، أو بعض صفحاته على موارد تخالف أو تتعارض مع: الشريعة الإسلامية، أو

[89] . ذهب علي جناتي، وزير الثقافة والإرشاد الإسلامي في الكابينة الوزارية للرئيس حسن روحاني في تصريح له بشهر مارس عام 2014 الى ضرورة رفع الحظر عن موقع التواصل الاجتماعي *Facebook* لأن عملية الحظر لا تزيد عن كونها معالجة سطحية، بينما يستمر أكثر من 4 ملايين مستخدم إيراني في الحضور بالفضاء التواصلي للموقع عن طريق توظيف أدوات الاحتيال السيبراني المختلفة. بالمقابل رأى الكثيرين ممن يستقرون في قمة البنية المؤسسية للمرجعية الدينية، ومؤسسة الحرس الثوري الإيراني ضرورة استدامة عملية غلق الموقع والتعامل بشدة مع المخالفين الذين يهددون ثقافة وانجازات الثورة الإسلامية في إيران (*Robertson&Marchant,2014*).

الأخلاق العامة، أو تشكل تهديداً للأمن الوطني، أو تنتقد الشخصيات الدينية والحكومية، أو تشجع على مقارفة الجرائم السيبرانية، أو ترشد المستخدم وتزوده بأدوات الاحتيال السيبراني (*Robertson&Marchant,2014*).

أما على صعيد المؤسسات ذات الصبغة التنفيذية، فتأتي في مقدمتها وزارة تقنية المعلومات والاتصالات فتتحمل مسؤولية تنفيذ عملية الحظر على القوائم التي تعد في هيئة تحديد الحالات، وفي الوقت ذاته تشرف الهيئة القضائية المرتبطة بالسلطة التنظيمية للاتصالات بإيران *Communication Regulatory Authority of Iran* (*CRA*) وبصورة مباشرة على التزام الشركات المجهزات للخدمة بسياسات الحظر التي تقوم بتحديد تفاصيلها هيئة تحديد الحالات *CDICC* وتقوم بتوجيه عقوبات رادعة للشركات المجهزة التي يثبت عدم التزامها بتفاصيل هذه السياسات أو إغفال بعض فقراتها. أما شرطة الفضاء السيبراني فتقوم بمهمة الكشف عن جرائم المعلومات واتخاذ الإجراءات بحق من يتلبس بها. ويقوم أفراد جيش الفضاء السيبراني الإيراني ومن التحق به من جنود الفضاء السيبراني المرتبطين بمؤسسة الحرس الثوري الإيراني في متابعة المحتوى المطروح في المواقع، والمدوّنات السيبرانية لتحديد المخالفات، ومباشرة هجمات رقمية مضادة لخلخلة عمل المواقع المناوئة لخطاب الثورة[90]، أو إغلاق صفحاتها (*Aryan, et.al.,2013*).

وعلى صعيد آخر تمارس وزارة الثقافة دور المراقب على محتوى صفحات الويب، حيث ألزم قانون جرائم الفضاء السيبراني *Computer Crime Law* (*CCL*) أصحاب مواقع الويب تسجيل مواقعهم لدى هذه الوزارة، ومنحها الحق في إجبارهم على رفع أي نص يتعارض مع توجهات الحكومة.

5 . 4 . 2 . سياسة روحاني باتجاه التقليل من الأغلال المفروضة على الفضاء السيبراني:

رغم ان إحدى أركان الدعاية الانتخابية لروحاني قد اكدت على مسألة حرية تداول المعلومات في إيران إلا أنه لم يستطع المباشرة بترجمة وعوده بعيد تربعه على منصب رئيس جمهورية إيران.

فقد وجد نفسه، منذ الأيام الأولى لتوليه الحكم، أمام تحديات كبيرة على صعيد تطوير بيئة فضاء الانترنيت، والتقليل من عدد سلاسل الأغلال التي اوغل الرئيس السابق محمود احمدي نجّاد في إحكام قبضتها على الفضاء المفتوح، ليحوّله شيئاً فشيئاً الى فضاء مكبّل.

لم تكن المهمة السهلة امام معارضين كثر، بعضهم قد تطاولت إقامته في شبكة النظام الذي تتحكم به مجموعة متداخلة من الهيئات، ومؤسسة الحرس الثوري التي تكاد تهيمن على كل صغيرة وكبيرة بالبلاد ويرى أن كل ما يرد من خارج البلاد يعد تهديداً للأمن القومي، والمرجعيات الدينية التي لا تقبل التساهل مع الثقافة الوافدة وتتعامل معها بحذر وتسعى الى منعها بالتحالف مع مؤسسة الحرس الثوري، أو البرلمان الذي يتقاسمه ممثلين عن هذه الفئات المهيمنة.

وقد استبق حضوره بعام واحد في تشكيل هيئة سلطوية للهيمنة على فضاء الانترنيت. ففي شهر مارس من عام 2012 وجّه المرشد الأعلى للثورة الإسلامية بإيران، علي خامنئي بإنشاء المجلس الأعلى لالفضاء السيبراني *Supreme Council of Cyberspace* (*SCC*) ليمارس دوراً فاعلاً في صياغة السياسات الوطنية لإدارة وتنظيم شبكة الانترنيت وخدماتها، واقتراح أفضل المعالجات لمراقبة السيل السيبراني المتدفق في فضائها، وحظر المواد التي تتعارض مع روح الثورة الإسلامية ومنظومتها الأخلاقية.

---

[90] . قامت مجموعة من جيش الفضاء السيبراني الإيرانية بهجمة في عام 2011 على أكثر من 300 ألف من مستخدمي الانترنيت بإيران ممن سعوا الى اختراق نظم الحظر وخالفوا التعليمات النافذة لاستخدام الانترنيت في البلاد (*Aryan, et.al.,2013*).

ورغم السجل الحافل لحفريات الانترنيت في البلاد الذي حفل بتجاذب الارادات وهيمنة القرار السياسي الذي دعمته المرجعية في حظر حزمة عريضة من مواقع الانترنيت، والتعامل مع فيضها السيبراني بوصفه تهديداً أكيداً لمكتسبات الثورة الإسلامية في إيران، وقناة يمكن للفكر المناهض أن يتسلل من خلالها الى البلاد، فقد أبدى الرئيس الجديد شجاعة نادرة وعزيمة أكيدة على مباشرة عملية إصلاح تستهدف إعادة تشكيل الخطاطة الوطنية للتعامل مع الفيض السيبراني للانترنيت، فصرّح في لقاء صحفي دعوته للمؤسسة السياسية والمرجعية دينية الى القبول بنهج التقليل من وطأة الحظر الذي يمارس على مواقع الانترنيت، لأنه لن يمنع المواطنين الإيرانيين من الدخول الى المواقع غير الأخلاقية ولكنه سيزيد من الفجوة التي تفصلهم عن الحكومة (*SMO,2015,a*).

ورغم الوعود التي قطعها على نفسه الرئيس روحاني، خلال حملته الانتخابية، فمن الملاحظ حصول طفرة نوعية على صعيد المراقبة السيبرانية على شبكات المعلومات والاتصالات بالبلاد منذ عام 2013، مع تغيير سياسات المراقبة والحظر وتصعيد إجراءاتها القمعية باتجاه تطبيقات الهواتف المحمولة أكثر مما هو الأمر عليه في مضمار مواقع الويب. وبدأنا نلحظ التحاق الكثير من التطبيقات التي تحفل بها مواقع هذه التطبيقات مثل *App Store* و*Google Store* بقائمة الحظر، بحيث لم يعد المستخدم الإيراني قادراً على الظفر بتطبيق تواصلي لم تناله كماشة الحظر(*SMO,2013,b*).

بيد أن هذه الأمور لا تلغي السعي الدائم للرئيس روحاني وبدعم من بعض أعضاء حكومته في مدافعة الدعوات التي ينادى بها في أروقة الحوزة ومؤسسة الحرس الثوري الإيراني، ومن إدارات المؤسسات الحكومية التي تنتمي الى دائرة الخطاب المتشدد، غير أنه قد حرص على المدافعة بنهج هادئ، وعبر خطوات تعتمد النهج طويل الأمد لضمان التخفيف من وطأة الأزمات المحتملة عن مثل هذه الإجراءات.

ولعل من الأمثلة البينة على سياسة روحاني الإصلاحية على صعيد التحفيف من ممارسات الحظر السيبراني، الخلاف الذي نشب مع هيئة تحديد حالات المحتوى الجنائي *CDICC* عندما رفعت طلباً الى وزارة تقنية المعلومات والاتصالات بحظر خدمة *WhatsApp* في نهاية شهر أبريل من عام 2014، بيد أن الوزارة قد وجهت لها اعتذاراً بعدم إمكانية إجراء عملية الحظر بناء على الأمر الذي وجهه رئيس الجمهورية روحاني بالتوقف عن حظر هذه الخدمة. واستمرت دعوات الحظر عندما صرّح عبد السلام أمد خرم آبادي (سكرتير الجمعية) أن رئيس الجهورية لا يمتلك صلاحية تجاوز قرارات جمعيته، وأن من واجب الوزارة القيام بحظر الموقع فوراً. بيد أن هذه الدعوات لم تثني روحاني عن قراره وأبلغ وزير تقنية المعلومات والاتصالات بعدم حظر الخدمة عن المواطنين الإيرانيين وعدم الالتفات الى مثل هذه التصريحات (*SMO,2015,a*).

وأسهمت مثل هذه القرارات في دعم وزير تقنية المعلومات والاتصالات على بيان تهافت ادعاءات أعضاء من الكابينة الحكومية للرئيس السابق أحمدي نجاد، وعدم الالتفات إليها. فقد حذر تاجي بور (وزير تقنية المعلومات والاتصالات في عهد الرئيس محمود أحمدي نجاد) من الوقوع بفخ استخدام تطبيق *Viber*، لأن مضيف هذه الخدمة موجود لدى الكيان الصهيوني، وأن بيانات الإيرانيين يمكن حفظها لدى اليهود واستثمارها في تهديد أمن البلاد، لذا أن ينبغي أن تتحلى الحكومة الإيرانية بالشجاعة والحزم في التعامل مع هذه التطبيقات، وتسارع بحظرها عن فضاء الاتصالات الإيراني، لأن وجودها يشكّل تهديداً أكيداً لقيم الدين وقيم الثورة الاسلامية. لذا حظرت كل من خدمتي *Viber &* *WhatsApp* للمرة الأولى في بداية عام 2013. وقد هرع محمد فايزي (وزير تقنية المعلومات والاتصالات في ولاية روحاني) الى بيان معارضته الصريحة لما ذهب اليه تاجي بور، وأن وزارته لا تفكر بحظر تطبيقات تبادل الرسائل لمنصات شبكات التواصل الاجتماعي (*SMO,2015,a*).

بالمقابل نلاحظ أن روحاني قد ينصاع باتجاه قبول بعض الدعوات الى حظر بعض الخدمات التواصلية، أو التطبيقات الشائعة، للتخفيف من وطأة التنازع مع جهات تمتلك بعداً مؤثراً في النسيج المعقد لصناعة القرارات، والتأثير على المجال السياسي والعقدي في البلاد. يحدث هذا عندما تختلط المبررات، في بعض الأحيان، لحظر هذه الخدمة أو تلك، أو تتباين الآراء بصدد الأرضية التي ترعرعت فيها نبتة الفكرة حتى صلب عودها وتولد عنها إجراء الحظر. ولعل من التطبيقات التي تقع في هذه الدائرة هو تطبيق *WeChat* الذي حظر في الربع الأخير من عام 2013 بناء على قرار صادر من هيئة الحظر *CDICC* (*SMO,2013,b*). فما أعلنته الهيئة لتبرير هذا القرار أشار الى أن هذا التطبيق، والذي تجاوز عدد مستخدميه من الإيرانيين 4 ملايين مستخدم، كان نتيجة لوجود دلائل أكيدة على ممارسة مجهز الخدمة عملية التلصص على البيانات والمعلومات الشخصية للمستخدمين، مع اختراق مكالماتهم.

بالمقابل ذهب آخرون الى أن سبب الحظر يعود الى رغبة الإدارة الحكومية بهجرة المستخدمين الإيرانيين من ساحة هذا التطبيق باتجاه التطبيق المحلي *Dialogue* والذي يوفر بيئة محلية يمكن إحكام عمليات المراقبة على كافة تفاصيل عمليات تواصل المستخدمين، من جهة، إضافة الى توافقه مع تطبيقات مشروع شبكة الانترنيت الوطنية *SHOMA*، من جهة أخرى. وذهب آخرون الى أن فرض عملية الحظر قد تمت بتوصية من قبل شركة إيران للاتصالات *TCI* بسبب توجه المستخدم الإيراني نحو استخدام هذه الخدمة المجانية، الأمر الذي حرم الشركة من الأجور المترتبة عن استخدام الرسائل القصيرة التي توفر عائداً مهماً للشركة الحكومية.

ورغم اعتراض جهات حكومية على إجراء الحظر، مثل إسماعيل أحمدي، قائد الشرطة الوطنية، وجهات حكومية متعددة، وأخرى من عامة الشعب، بسبب سهولة الاستخدام وعدم وجود مبررات راسخة لعملية الحظر، إلا أن الهيئة أصرّت على ما ذهبت إليه، فنفذت قرارها واستبعدت هذه الخدمة الاتصالية عن دائرة تواصل المستخدمين الإيرانيين عبر هذا الموقع الشعبي.

ولم تتوقف عملية التدافع والتجاذب على صعيد الهيمنة على مجال قرارات الحظر، بعد أن أضحت هذه المسألة جزءاً لا يتجزأ من ملف الأمن الوطني للبلاد، ومدخلاً لحماية بيضة الثورة الإسلامية وثقافتها، من أجل هذا يسعى الكثيرون من أعضاء المجلس الإيراني، وقيادات في الحرس الثوري، ومجموعة من المتشددين في النظام القضاء الإيراني، والمؤسسة الحوزوية إقصاء الحكومة عن دائرة صناعة القرارات الخاصة بإدارة الفضاء السيبراني وضمان أمنه، وحصرها بهيئة *CDICC*، حرصاً منهم على استبعاد الخطاب المعتدل الذي لهج به الرئيس حسن روحاني، ولاستبقاء القيود الصارمة إزاء توظيف هذا الفضاء في إنتاج خطاب إيراني بديل للخطاب الذين ينادون به. وقد تزايدت الضغوط التي باشرها الكثير منهم، بصورة مباشر (عبر ممثليهم المتواجدين على طاولة المجلس الأعلى لالفضاء السيبراني) من جهة، وبصورة غير مباشرة عن طريق تأجيج أصوات المعارضين لكل خطوة يحاول من خلالها الرئيس إزالة بعض القيود، أو تبني تشريعات جديدة أقل غلواً[91].

وصفت الإجراءات التي اتخذتها حكومة روحاني للتقليل من مساحة الحظر المفروضة على مواقع الانترنيت ومحتواها السيبراني، بالمحاولة المتواضعة، ذلك لأن مشروع حظر المواقع وترشيح المحتوى الذكي، ورغم وعود الإدارة الحكومية بممارسته دوراً فاعلاً بالتقليل من وطأة الحظر الصارم الذي يمارس على مواقع فضاء الانترنيت امام المستخدمين الإيرانيين، لم يمارس معالجاته سوى على مواقع التواصل الاجتماعي في مرحلته الريادية *Pilot Stage* مع إطلاق وعود

---

[91] . عمد النائب العام الإيراني، صديق لاريجاني، الى توجيه سهام النقد، وبصورة غير مباشرة، الى سياسات الرئيس روحاني على صعيد إدارة خدمات الانترنيت بالبلاد، ونبّه على ضرورة التزام السلطات الإيرانية بالحذر تجاه أنشطة المعلومات والاتصالات والتي باتت تشكل خطراً أكيداً على النظام الإيراني، مؤكداً على ضرورة حصر سياسات الحظر والمراقبة بهيئة *CDICC* مع منحها استقلالية تامة عن دائرة الهيمنة الحكومية (*F.H,2015*).

حول قرب رفع الحظر المفروض على مواقع التواصل الاجتماعي (*Facebook, Twitter, Instagram, You Tube*) والتي لم تتحقق حتى هذا التاريخ[92].

لكن بدورنا نود أن ننصفه فنقول، أنه رغم أن الإصلاحات التي يمارسها الرئيس روحاني، لا زالت تبدو محدودة للعيان، وتعاني من تعثرات متعددة، إلا أنه لا زال مستمراً بالتنقير عن سبل أكثر نجاعة، تسهم في خلخلة الاتجاهات المتشددة. نذكر منها نجاحه في تقليص الصلاحيات به المطلقة لهيئة *CDICC* في فرض توجهاتها من خلال اعتماد نظام داخلي يمنحها فرصة المصادقة على قرارات أعضائها المتشددين متى صوّت خمسة أعضاء من مجلسها على المقترحات المطروحة على طاولة اجتماعاتها، وذلك بإحداث تعديل يربط المصادقة بالإجماع المطلق لأعضاء الهيئة،[93] الأمر الذي بات يشكّل عقبة كبيرة أمام الموافقة على قراراتها المتشددة والمغالية في فرض الحظر على المواقع، أو تقطير مادة المحتوى السيبراني.

كذلك فإن اعتماد إدارة روحاني سياسة توظيف نظام الحظر والترشيح[94] الذكي لحظر الصفحات التي تضم بين ثناياها محتوى محظوراً بدلاً من حظر جميع محتوى الموقع، يمكن أن يعد خطوة إيجابية للتقليل من المساحة التي تمارس في حظر المواقع بفضاء الانترنيت في إيران. وقد حدد سقفاً زمنياً قدره 10 أشهر لإكمال مشروع الحظر والترشيح الذكي بمراحله الثلاثة. وقد استغرقت المرحلة الأولى شهراً واحداً، بينما خطط للمرحلة الثانية مدة ثلاثة أشهر، بينما توقع أن تستغرق المرحلة الثالثة ستة أشهر.

وقد استكملت المرحلة الأولى في شهر يناير من عام 2015، بينما بوشر العمل على المرحلة الثانية في شهر آذار من العام ذاته[95]. وكان من أهداف المرحلة الأولى ضمان قيام النظام بتقطير محتوى الصور المودعة في موقع التواصل الاجتماعي *Instagram* بالإضافة الى تقطير محتوى صفحات موقع *Facebook*. وقد ادعى الوزير الإيراني أن نظامهم أثبت قدرته على ترشيح 83 % من مادة المحتوى المحظور في هذين الموقعين خلال عمليات الاختبار التي أجريت عليه[96].

---

92 . راجع: المقال المنشور على الموقع, ***Iran's New 'Smart' Internet Censorship Efforts Still Aren't Particularly Smart***, *https://www.techdirt.com/articles/20150106/.*

93 . يوجد ضمن أعضاء مجلس هذه الهيئة ثلاثة عشر عضواً من الكابينة الحكومية للرئيس روحاني تكاد أن تتطابق توجهاتهم مع سياسته الإصلاحية والمعتدلة.

94 . وقد اقترحت الإدارة، هذا الأسلوب من المعالجات في بداية شهر نوفمبر من عام 2014.

95 . تناقض وزير المعلومات والاتصالات الإيراني، فايزي، في تصريحه حيث ذكر أن المرحلة الثالثة قد بوشر بها في 21 آذار من عام 2015، في حين ذكر في تصريحه للصحيفة ذاتها أن المرحلة الثانية ستستغرق ثلاثة أشهر وأنها قد بدأت في بداية الشهر آذار ذاته؟.

96 . ورد التصريح في صحيفة *Financial Tribune Daily*، أنظر الرابط: ***3rd Phase of Smart Filtering***, *Financial Tribune Daily, October 18, 2015,*

http://financialtribune.com/archive/2015/10/18/articles/economy-sci-tech/14191/3rd-phase-smart-filtering

الفصل الرابع:
فضاء النزاعات والتهديدات والحروب الناعمة

الفصل الرابع: فضاء النزاعات والتهديدات والحروب الناعمة

1 . إعادة مراجعة مفهوم الفضاء السيبراني:

بعد أن نجح ببسط هيمنته على فضاء حيواتنا وأنشطتنا الأرضية، كثر الحديث في مجال تحليل عناصر الفضاء السيبراني والكشف عن هويته الأنطولوجية، فتكاثرت المصطلحات التي اقترحت لوصف هذا الفضاء الجديد، حتى تداخلت المفاهيم، وتعددت الرؤى، وامتد تأثيرها الى ساحة معالجة ماهية الكيانات، التي استحدثت بذورها الفريدة من مادة خطاطته المعرفية، واستنبتت في تربته السيبرانية الخصبة.

في عام 1982 قام ويليام جيبسون، أحد الكتاب الانجليز المتمرسين في حقل أدب الخيال العلمي، بنحت مصطلح *Cyberspace*، في محاولة لتلبية عوز احداث روايته الشهيرة *Neuromancer* الى مصطلح فريد يعبّر عن حضور لنسق وجودي جديد، يتوافق مع الخطاطة التي حاول أن يصطنع أحداث حبكته الروائية لمعالجة بعض مسائلها (الرزو،2008).

ولد اصطلاح *Cyberspace* لدى جيبسون عندما عمد الى استعارة الشق الأول من اصطلاح *Cybernetics* (الذي لم تنضج بعد دلالاته العلمية والاصطلاحية)، *Cyber*، فألصقها مع مصطلح *Space*، فنتج عن هذه الجمعية الاصطلاح الجديد. لم تكن عملية صناعة المصطلح عفوية، وإنما جاءت لتضفي سحراً، وشيئاً من الغموض، لحضور بصمة من علم السبرنتيك الذي فتح الباب أمام حزمة من التقنيات والتطبيقات العلمية والتقنية الواعدة، من جهة، وحضور مصطلح الفضاء الذي رغم شيوع استخدامه، لا زال يوحي بمجالات متخيلة، ومنفتحة، على أحياز، تتجاوز في كثير من الأحيان تصوراتنا، رغبة من في منح مصطلحه الجديد، انفتاحاً وسعة تتناسب مع خطاب الخيال العلمي، الذي يحرص على خلق جو تصوري يأخذ بألباب القراء، ويشدّهم نحو عوالم سحرية، لا نكاد نعثر عليها إلا في ساحة أحلامنا وخيالاتنا الجامحة.

لم يخطر ببال جيبسون، ولو لبرهة من الزمن، أن المصطلح الذي اصطنعه لتلبية رواية قصيرة من روايات الخيال العلمي، سيكون له شأن بحيث تنصبغ بدلالاته مجموعة متنوعة من الأنشطة والتقنيات، لا بل ينصبغ به ويلتصق ببنيته الاصطلاحية عصر يعد من أكثر العصور في تاريخ البشرية، ثراء في إنتاج المفردات المعرفية، ومعالجتها، وإعادة توليدها.

1 . 1 . الارهاصات التي أسهمت ببزوغ مصطلح *Cyberspace*[97]:

في البداية، وفي منتصف عقد الستينات من القرن العشرين بالتحديد، لم يكن هناك ثمة *Cyberspace* وإنما مجموعة حواسب طرفية *Terminal Computers*، كانت تستخدمها وزارة الدفاع الأمريكية (البنتاغون) لإدارة أنشطتها البحثية واللوجستية. وقد تولدت قناعة لدى مؤسسة مشاريع البحوث العسكرية المتقدمة *Advanced Research Projects Agency (ARPA)* بضرورة دعم أنشطة الباحثين من خلال إتاحة فرصة وصول الى البيانات المتوفرة في حواسب بقية الباحثين، من خلال أي لوحة طرفية، متجاوزة عقبة الرقعة الجغرافية التي تتواجد فيها تلك اللوحة، مع تجاوز التباين في نظم التشغيل التي تستخدم في إدارة النظام السيبراني.

كان هذا المشروع البحثي، سبباً في ولادة مشروع شبكة *ARPANET* التي تمثل نقطة الشروع الأولى باتجاه بناء شبكة الانترنيت الحالية. وكان فضاؤه محدوداً ضمن الرقعة الجغرافية للولايات المتحدة الأمريكية، حيث انتشر الباحثون

97 . حرصت على إيراد الاصطلاح كما ورد باللغة الإنجليزية من الفقرة الأولى، وعدم ايراد الاصطلاح باللغة العربية لحين انجلاء الغموض عن دلالته، وانتخاب مصطلح مناسب له من لغتنا العربية، بحيث يتوافق مع مضامينه المعرفية والتقنية.

الملتحقين بمراكز بحوث البنتاغون، كان مجال الفضاء الجديد مقتصراً على بضعة حواسب، وبعدد مناظر من المواقع (*Jordan, 1999*).

كانت الغاية الأساسية من إنجاز هذا المشروع تكمن في تجاوز عقبة المسافة المتسعة التي تفصل بين الوحدات البحثية المنتشرة في عموم الولايات المتحدة الأمريكية، وتعزيز الأنشطة البحثية وما يصاحبها من عمليات تمويل اقتصادي، بيد أن المراجعة الأولية للفيض الاتصالي الذي تدفق بين حواسيب هذه الوحدات والمراكز التي التحقت بالمشروع خلال عقدين من الزمن (والتي بلغ عددها 150 موقعاً عند نهاية عام 1980)، أظهرت أن أكثر من75% من هذه الأنشطة قد استثمرت الشبكة الالكترونية لتبادل الرسائل عبر خدمة البريد الالكتروني.

أنشئت العقدة الشبكاتية الأولى لمشروع *ARPANET* عام 1969 في جامعة *UCLA*، ثم تزايد عددها عند نهاية العام ذاته فبلغت 4 عقد شبكاتية، ثم أنشئت المزيد من العقد الشبكاتية ليبلغ عددها عام 1971، 15 عقدة، وستمر توسع استخدام شبكات المشروع فبلغ عددها عام 1973 حوالي 37 عقدة انتشرت في أماكن متفرقة بالولايات المتحدة (*Denning,1989*).

وجاءت ولادة خدمة البريد الالكتروني عام 1971 على يد *Ray Tomlinson*، ورأى النور في العام ذاته مشروع جوتنبرج لتوفير الكتب الالكترونية بالمجان على شبكات المعلومات.

ثم بدانا نشهد مشاريع مشابهة لمشروع *ARPANET* في دول أخرى، فنجحت فرنسا بإحداث حاول محاكاة الشبكة الأمريكية أطلقت عليه اسم *CYCLADES* لكنه لم يكتب له النجاح، فقد توقف عن العمل بعد مدة قصيرة، نتيجة لبروز مشاكل تقنية جمة.

وبدأ مشروع *ARPANET* بتوسعة قنواته الاتصالية، بعد أن امتد نسيجه على مساحة واسعة من الولايات المتحدة، فأنشئت عقدة الترابط الأولى عبر الأطلسي عام 1973، فارتبط نسيجه الشبكاتي بعقدة معلوماتية مع جامعة لندن.

ولم تعد المعمارية الشبكاتية، الحرجة، التي اتسم بها المشروع، تفي بالتوسع الذي طرأ على خدمات الشبكة، وامتداد رقعتها الجغرافية، قادرة على تلبية سمة التعقيد التي بدأت تسري في نسيجها الشبكاتي، فبرزت نداءات جديدة دعت الى إحداث المزيد من الشبكات التي تحاكي أداء شبكة مشروع *ARPANET*، وأطلق عليها مصطلح شبكات متشابكة *Inter-Network* بحيث يغيب عن هيكلتها خاصية الإدارة المركزية، التي باتت تحد من حرية وفرص انتشارها. وقد أسهم ابتكار بروتوكول *TCIP/IP* الذي رأى النور عام 1974 بتحويل الحلم الى حقيقة، وأعلن عن ولادة معمارية شبكاتية، تتسم بمرونة عالية، وانفتاح على مجموعة الشبكات التي التحقت بنسيجها، فكانت بداية حضور شبكة الانترنيت. وقد تجاوزت المعمارية الجديدة المحددات التي ألزمت شبكة *ARPANET* بعدد لا يتجاوز 1000 مضيف الكتروني *Host*، فبلغ عدد مضيفات الانترنيت عام 1987 ما يقارب 30,000 مضيف. فازداد فضاء الفيض السيبراني لشبكة الانترنيت اتساعاً، بعد ازدياد عدد المضيفات، والعقد الشبكاتية التي ترتبط بها (*Sutherland,2000*).

ثم جاء الابتكار الذي حوّل شبكة الانترنيت من شبكة لا تحسن التواصل سوى بالنصوص الصماء، الى شبكة ثرية بمواد الوسائط المتعددة، وتمتلك مواقع تناظر في بنيتها معمارية الواقع. إنه الابتكار العبقري الذي اقترحه *Tim Berners-Lee* عام 1989 وأطلق على نظامه مصطلح الشبكة العنكبوتية العالمية *World Wide Web*، وأنشئت بموجبه أول صفحة لموقع ويب عام 1991.

وحينئذ ولد فضاء متخيّل جديد لم يفلح العاملون في ميدان تقنية الانترنيت في إيجاد مصطلح يقارب تزاوج ثراء المحتوى، وغموض مضامين البيئة السيبرانية الجديدة، ومضاهاتها الحذرة للواقع سوى المصطلح الذي جاء به وليم جيبسون، فهرعوا الى تعريف فضاء الفيض السيبراني الذي بدأ يتمدد داخل النسيج الشبكاتي للانترنيت، وجعلوا من

مصطلح *Cyberspace* الوصف الذي سينهض بمهمة التعبير عن البيئة الفريدة التي أحدثت زلزلة، وطفرة مفاهيمية غير مسبوقة.

1 . 2 . ولادة كلمة *Cyberspace* في قاموس روايات الخيال العلمي:

تحفل قواميس روايات الخيال العلمي بعدد كبير من المصطلحات والكلمات المستحدثة التي ابتكرها ادباء وروائيو هذا الأدب (*Frank,2009*). بيد أن الكثير من هذه المصطلحات لم يكتب لها فرصة الخروج من نصوص الروايات والقصص التي ولدت فيها، بالمقابل كتب لبعض المصطلحات أن توظف في خارج حدود الأدب، وتستوطن في دائرة العلوم والاستكشافات الحديثة.

وتعد رواية *Neuromancer* للروائي وليم جيبسون[98] (*Gibson,1984*) من اول لأعمال الروائية التي حازت بجدارة على جائزة التاج الثلاثي لأدب الخيال العلمي (جائزة *Nebula Award*، وجائزة *Philip Dick Award*، وجائزة *Hugo Award*)[99].

ولم تقتصر بصماته الأدبية على مجال أدب الخيال العلمي، فقد ابتكر جيبسون في سياق الرواية مجموعة متنوعة من الكلمات التي صاغها من الحصيلة اللغوية التي اودعت في المعاجم التقنية، فاصطنع كلمات ومصطلحات فريدة، شدّت انتباه القراء لغرابتها، وكانت مصدر وحي وإلهام للعاملين في حقل محيط المعلومات وتطبيقاته التي تتسم بسمة افتراضية.

مارست هذه الرواية الخيالية دوراً كبيراً في تشكيل الكثير عناصر خطاطة المجال المعرفي لمحيط المعلومات، وفضائه السيبراني المتخيّل. كما ألهمت مجموعة كبيرة من العلماء، والمفكرين والأدباء، والفنانين بأفكار تحوّلت، شيئاً فشيئاً، الى منتجات معرفية، وظّف بعضها داخل حدود خطاطة المعلومات والاتصالات، بينما أنتجت أخرى تقنيات استجمام مبتكرة، واستخدمها آخرون في تشكيل مفاهيم فريدة، أودعت في أفلام الخيال العلمي التي أحدث حضورها ضجة كبيرة خلال العقد الأول من القرن الحادي والعشرين.

فكان حضور مصطلح المصفوفة *Matrix* في روايته مصدراً للإرهاصات العلمية التي أحدثت شبكة الانترنيت وعقدها السيبرانية، وكلمة *Nexus* ليصف من خلالها الروابط التي تصل بين الحواسب وعقد المعلومات، والتدابير الإلكترونية المضادة للاختراق السيبراني *Intrusion Countermeasures Electronics* التي تحولت الى نشاط تمارسه منظومة أمن المعلومات في البنتاغون.

ولم يقتصر عمل جيبسون على هذه المصطلحات، بل عكف على اصطناع مصطلح آخر، شاءت الأقدار أن يشكل نواة لعالم متخيّل يوازي الواقع الذي نعيش فيه. إنه مصطلح *Cyberspace* الذي كتب له أن يلتصق بأكثر من مادة وفكرة ابتكرت خلال عصرنا الراهن، ونجح بأن يكون المفتاح الجوهري لمجموعة من المصطلحات التي غزت فضاء الانترنيت، وبيئته السيبرانية المعاصرة.

اصطنع وليم جيبسون مصطلحه الجديد من كلمتين، الأولى كلمة *Cyber* والتي استعارها من ميدان علم السايبرنتيك[100] *Cybernetics*، اما الثانية فكلمة *Space* التي تعددت معانيها، واستوطنت أكثر من حقل من حقول

---

[98] . وليم جيبسون *William Ford Gibson* أديب أميركي من أصول كندية، من أعمدة أدب الخيال العلمي الحديث. تعد روايته الشهيرة *Neuromancer* (التي صدرت عام 1984) مورداً مهماً لكثير من المصطلحات التي أضحت مورداً مهماً أوحت للعاملين في مجال السيبرانية والاتصالات بالكثير من عناصر الخطاطة المعرفية السيبرانية. لمزيد من المعلومات عن حياة هذا الأديب يمكن مراجعة المقال الموجود على الموقع: *http://en.m.wikipedia.org/wiki/William_Gibson*.

[99] . *http://williamgibson.wikia.com/wiki/Neuromancer*.

[100] . السايبرنتيك علم يعنى بدراسة تكامل النظم الميكانيكية، أو الفيزيائية، أو الحيوية، أو الإدراكية ضمن خطاطة تنتج حلقة تأثيرات تحاكي سريان الأحداث في حياتنا اليومية، وتمنحنا فرصة التحكم بمسالك نتائجها.

المعاجم العلمية والأدبية على حد سواء. فنشأ عن هذا التزاوج اللفظي كلمة جديدة لا نكاد نعثر على كلمة مرادفة لها في قواميس اللغة هي كلمة *Cyberspace*.

ارتبط معنى الكلمة الجديدة وحضورها المؤثر في روايته الشهيرة *Neuromancer* بنمط من التصوّرات والخيالات التي تقارب أن تكون عبارة عن هلوسة توافقية يعيشها، كل يوم، عدة مليارات من المشغلين المنطقيين، في كل شعب من الشعوب... وهو نمط من التمثيل الرسومي لحزمة من البيانات المجرّدة، التي استمدت من مستودعات البيانات لكل حاسب يستوطن في المنظومة الإنسانية. ويتميز بتعقيد لا يمكن تصوّره، أو تمثّله بآلة استدلالنا العقلية.

وتتألف مادة هذا الفضاء الافتراضي من حزم ضوئية تتراصف في العقل ضمن المنطقة التي تخلو من البعد المكاني، حيث تتشكل عناقيد البيانات وكويكباتها المجردة.

وصف يتوافق الى حد كبير مع الأفكار التي تحفل بها روايات الخيال العلمي، يسوده تجريد واضح، مع محاولة لاصطناع فضاء مفاهيمي، يسحب القارئ الى تيه يخلو من المعنى، ويمكن أن يتقبل لأي نمط من أنماط الهلوسة التي تغزو فضاء الحلم الذي نحلق فيه عندما نخلد الى النوم كل يوم.

من أجل هذا فليس بمستغرب أن نجد، وللمرة الأولى، إقرار مبتكر المصطلح، بأنه لم يكن على علم ودراية بماهيته، وأن ولادته كانت غير متعمدة، وأنه حضر في لحظة من لحظات الالهام الذي سكن قريحته الأدبية عند كتابة الفقرة التي انبثق فيها.

وقد آثرنا إيراد تعليقه على مصطلحه الفريد، حيث يقول[101]: **" كل ما أعرفه عن كلمة *Cyberspace* عندما قمت بصياغتها، أنها كلمة طنانة، تلتصق بالذاكرة، بسهولة، رغم خلوها من المعنى. أحسست في وقتها، أنها توحي بشيء ما، رغم خلاؤها من أي مدلول حقيقي، حتى بالنسبة لي، عندما عايشت بروزها بين الكلمات التي استوطنت الصفحة التي كانت تقبع أمامي".**

لقد ولدت الكلمة عند جيبسون لتحقيق رغبة مستبطنة في إحداث كلمة طنانة، تشدّ القراء إليها وتصطنع في مخيلتهم فضاءً متخيّلاً من نمط فريد، نتيجة للغموض الذي يلفها، بفعل صياغتها من كلمتين لا تمت إحداهما الى الأخرى بصلة واقعية، والتصاقها بعلم جديد لا زال يعد بإمكانية استحضار عتبة للتناغم بين نظم التحكم الميكانيكي، والذات البشرية، لإنتاج كينونة هجينة، تتسم بسلوك مستغرب.

وقد شاع استخدام المصطلح الجديد، ووجد قبولاً عند الكثير، لا لشيء إلا لغرابته، واستخدامه في وصف أكثر الظواهر التي أحدثت نقلة مفاهيمية في خطاطتنا المعرفية، شبكة الانترنيت، وبيئتها الافتراضية التي بدأت تتحدى عناصر الواقع، ونجحت في جذب الانسان المعاصر من الواقع الفيزيائي الى الواقع المتخيّل.

وبدأنا نعايش ولادة مجموعة متنوعة من الكلمات والمصطلحات التي استعيرت فيها كلمة *Cyber*، وبوركت عملية تزاوجها المعلن مع الكثير من المصطلحات والكلمات الشائعة، لتحوّلها من بيئتها التقليدية الى بيئة تلتصق بتقنيات المعلومات والاتصالات، حيث البيئة الاتصالية المتخيّلة، والفيض السيبراني الذي يملأ فضاءها بمساراته المتواشجة، وعقد نسيجه الشبكاتي، الذي يتسم بميزات افتراضية فريدة.

---

[101] *William Gibson*, quoted in The Economist, December 4, 2003 .[128].

ومن هذه البنيات اللغوية الجديدة، ثقافة عصر المعلومات *Cyberculture*، والتهديدات السيبرانية *Cyberattacks*، والفن السيبراني *Cyberart*، ورجل الفضاء السيبراني *Cybernaut*، وحروب الفضاء السيبراني *Cyberwarfare*، وغيرها من الكلمات التي بدأت تتوالد على التوازي مع الحضور المتسارع لأدوات المعلومات وتقنياتها في حياتنا المعاصرة[102].

1 . 3 . التحاق مصطلح *Cyberspace* بحياض السيبرانية:

ولدت شبكة الانترنيت، واختمر جزء لا بأس به من معماريتها السيبرانية، قبل ولادة مصطلح *Cyberspace* والذي جاء متأخراً عن ولادتها بحوالي عقدين من الزمن. ولعل المبرر لهذا التأخير، وخلو الخطاطة السيبرانية للانترنيت من وصف لفضائها المستحدث، مرتبطاً باحتكار استخدامها لدى المؤسسة العسكرية بالولايات المتحدة الأمريكية، وبضعة مراكز بحثية، ومؤسسات جامعية، أنكب فيها العلماء والباحثون على تلمّس قدرات شبكة الحواسب على التواصل، ونقل رسائل البريد الالكتروني، التي لم تختلف كثيراً عما ألفوه من القدرات التي تميزت بها شبكات الهاتف والتيليغراف.

بيد أن الطفرة التي أحدثها مفهوم الشبكة العنكبوتية العالمية وقدرتها على اصطناع مجال يقارب الوصف المكاني لفضاء رقمي، يحتوي على مواقع ويب، تنتشر على مساحة واسعة من نسيج شبكاتي يحاكي بنية الشبكات الاجتماعية *Social Networks* التي نادى بها علماء الاجتماع المعاصرين، كانت سبباً مباشراً للتنقير عن مصطلح جديد، يتسم بفرادة وخصوبة غير مسبوقة، ويمتلك بالوقت ذاته، مرونة مفاهيمية، قادرة على استيعاب التغييرات المتسارعة التي تسري في كيان وتطبيقات الفضاء المفتوح لشبكة الانترنيت.

من جهة أخرى، ارتكز التصور الخيالي لكلمة *Cyberspace* لدى وليم جيبسون الى وصف مجال يضم في فضائه جميع المفردات السيبرانية التي أنتجها الكائن البشري، والتي يمكن تغذيتها الى دائرة الوعي غير المتجسد، من خلال الفضاء السيبراني الذي يتولّد داخل حدود بيئته وتطبيقاته البرمجية. ويعد الفضاء الجيبسوني (الذي اقترحه وليم جيبسون في روايته *Neuromancer*) مصدر قوة للكيانات التي تمتلك القدرة على معالجة البيانات المستوطنة فيه، بمهارة وحنكة. ويلتحق بهذه الفئة قراصنة المعلومات، والمؤسسات التي تمتلك معرفة رقمية راسخة (*Jordan, 1999*).

وقد صاغ جيبسون اصطلاح *Cyberspace* لكي يولّد لدى قرائه تصويراً مجازياً يتسم بطابع مكاني، رغم قناعته بغياب الخاصية المكانية عن النسيج الشبكاتي للحواسب الذي عالجه ضمن خطاطة الخيال العلمي لروايته الشهيرة *Neuromancer* . ونجح بزج هذه الاستعارة في وعينا الباطن، فتعمّق لدينا الاعتقاد بتحيّز فيض المعلومات المتدفقة بين عقد الحواسب، والنسيج الشبكاتي في فضاء رقمي من نمط فريد.

أعلنت موسوعة *Wikipedia* السيبرانية أن اصطلاح *Cyberspace* قد استخدم للمرة الأولى، عام 1990، لوصف الفضاء السيبراني الذي اكتظ بمواقع الانترنيت، بعد أن شاع استخدامها، وتكاثرت تطبيقاتها الواعدة في البيئة الاتصالية ـ السيبرانية (*Wikipedia,2015*).

حينئذ حصلت الولادة الثانية للمصطلح، بعد حوالي عقد من الزمان من الارهاصات الأدبية التي دفعت وليم جيبسون الى اصطناعه في رواية من روايات الخيال العلمي، وكتب لهذه الكلمة الخالية من المعنى، ولصاحبها، أن تحتل مساحة غير مسبوقة، على صعيد اهتمامات الانسان المعاصر، بعد ان استعيرت الى مجال شبكة الانترنيت، فأنجبت الكثير من الكلمات والمصطلحات التي استعارت جزءاً من بنيتها اللغوية لتصطنع المزيد الفضاءات المفاهيمية التي عبّر عنها بأدوات أو آليات اتصالية استوطنت فضاء الانترنيت.

---

102 http://project.cyberpunk.ru/idb/dictionary.html. .

وقد جاء حضور مصطلح *Cyberspace* بوصفه وصفاً لفضاء الانترنيت، في قواميس اللغة الإنجليزية، متأخراً، بعد أن شاع استخدامه ضمن بنيات متعددة من الاستعارات اللغوية، التي تجاوزت حدود الفضاء السيبراني، باتجاه وصف الكيانات الفريدة، التي ولدت نتيجة لتوسع مجال استخدام أدوات المعلومات والاتصالات.

وتظهر المراجعة المتأنية لدلالة هذا الاصطلاح وجود لبس بالمفهوم، مع تلمس محاولة حثيثة من اللغويين الذين أعدوا المادة اللغوية والعلمية لهذه المفردة في إيراد معاني متعددة للمفهوم، بيد أن هذه المحاولات الجادّة لم يكتب لها النجاح في التوفيق بين الدلالة التي تكمن في البنية المعجمية للمصطلح، من جهة، والمحمولات التي استعيرت من قاموس تقنية المعلومات والاتصالات، من جهة أخرى.

من أجل هذا لا تكاد تعثر في هذه القواميس على ما يشفي الغليل، ويكشف اللثام عن معنى المصطلح، الذي ارتبط بالوسط الالكتروني الذي ينشأ عن أنشطة الاتصالات السيبرانية التي تسافر في فضاء شبكات الحواسب، والتي تلتحق بنسيج شبكة الانترنيت.

ونلاحظ في بعض القواميس، محاولات لإزالة الغموض عن دلالة المصطلح، وذلك من خلال مقاربته مع مصطلح الواقع المتخيّل *Virtual Reality* والذي يختلف في ماهيته، الى حد كبير، عن ماهية *Cyberspace*[103].

إن التحاق المصطلح في بيئة المعلومات والاتصالات، وهيمنته على وصف فضائها، والتصاق جزء من بنيته اللغوية بالكثير من المصطلحات التي ولدت لمواكبة التقنيات الجديدة التي استوطنت البيئة السيبرانية، بات يشكّل تحدياً لنقل المصطلح الى القواميس العربية، ولغة خطابنا العربي. وقد هرع البعض الى استخدام مصطلح الفضاء السيبيري، لتجاوز عقبة التعامل مع مصطلح علم السايبرنتيك، بينما ذهبت مع آخرين الى استخدام اصطلاح الالفضاء السيبرانيي لوصفه بلغتنا العربية (الرزو،2007)، وجاء آخرون فأطلقوا عليه اصطلاح الفضاء الافتراضي.

بيد أن معالجتنا الراهنة لولادة المصطلح، وتتبع آثار نمو دلالاته، وتحديد زمن التحاقه ببيئة الانترنيت قد حتّم عليَ معاودة النظر بما يناسبها من الألفاظ العربية، فوجدت أن أكثرها قرباً هو **فضاء الفيض السيبراني**.

وعلى هذا الأساس، يمكن أن نتصور فضاء الفيض السيبراني بوصفه شبكة، او مصفوفة رقمية من العقد السيبرانية التي تنتشر على عموم النسيج الشبكاتي الذي تلتحم بلحمته جميع الحواسب القاطنة في مجال الحوسبة العولمي، ويتشكل عن ترابطها، وتواصلها مجال تقطنه البيانات التي تسري نتيجة للنشاط السيبراني الذي يمارسه المستخدمون.

ويتميز هذا المجال بغياب الخاصية المكانية عن الساحة التي يستوطن فيها، وينبثق عنها حضوره، ولا يمكن تمثّل أنطولوجيته الوجودية إلا عند ممارسة أنشطة التواصل والتفاعل عبر مرقاب الأداة السيبرانية (حاسوب كان أم أداة اتصال ذكية)، حيث يترعرع في المناخ السيبراني التواصلي جملة من المؤثرات المرئية التي تعزز انتماء المستخدم الى مجال شعوري، تغيب فيها البصمة المادية لجسده، وتصاعد دور الشعور في تأكيد حضوره بفضاء يتجاوز محددات الزمان والمكان، ويرسخ إحساسه بكينونة وجودية، من نمط فريد، توازي (في بعض سماتها) حضوره المادي على أرض الواقع الملموس.

وقد عززت العبارات (التي نستخدمها أثناء حضورنا في فضاء الانترنيت)، الدور الأنطولوجي للفضاء الجديد. فقد شاع استخدام الكثير من العبارات عند تعاملنا معه، مثل: الانتقال الى صفحة الويب، الدخول/ الوصول الى الموقع، الإبحار

[103] . يمكن مراجعة هذه المجموعة من القواميس للوقوف على المعاني التي اقترحت لبيان معاني المصطلح:

Online Etymology Dictionary, (2010), The American Heritage, Science Dictionary, (2002), The American Heritage, New Dictionary of Cultural Literacy, (2005), The Dictionary of American Slang, (2007), The Free On-line Dictionary of Computing, (2010), Collins English Dictionary – Complete and Unabridged, (2003), Dictionary of Military and Associated Terms, (2005).

بين مواقع الانترنيت، وغيرها كثير...)، والتي توحي بممارسات ذات بعد مكاني، مما أسهم شيئاً فشيئاً، بتوطيد نمط جديد من الحضور الانطولوجي الذي بات يولّد لدينا الإحساس بفضاء مجرّد، غير أنه يتسّم بحضور مكاني ما انفك ملتصقاً بجوهر يمتلك خطاطة جغرافية تخلو من عنصر المكان!.

ويحتوي هذا الفضاء الشامل، على مجموعة من الفضاءات الثانوية التي تنتجها مختلف أنماط التطبيقات، ومواقع الويب، والتي تسري في مجالها الاتصالي، الفيض السيبراني الذي ينتجه المستخدمون اثناء تفاعلهم مع محتوى التطبيق، أو بقية المستخدمين الذين يتواصلون، ويتفاعلون معهم.

وتتوافق خصائص هذا الفضاء، الى حد كبير، مع المفاهيم المجرّدة، والدلالات الرياضية والمنطقية التي تجاوزت عقبة الخطاطة الإقليدية باتجاه فضاءات جديدة لا إقليدية، باتت تبتعد عن الفضاء الفزيائي الذي تتطابق خطاطته مع تفاصيل ممارساتنا اليومية.

فلا تتوفر بين أيدينا أداة، أو معايير قادرة على قياس حجم الفضاء السيبراني، ومراجعة عمليات النمو أو الانكماش الحاصلة في مجاله، ولا زالت المعايير تعتمد على عدد العقد السيبرانية، ووفرة أدوات المعلومات والاتصالات، وتزايد أعداد المستخدمين، أو تناقصهم، وهي معايير لا تتوافق مع الوصف الفيزيائي للفضاء الذي تتحكم به مجموعة من العوامل الفيزيائية. ويختلف زمن وصولنا الى موقع ما، نتيجة وفرة قنوات التواصل مع المضيف، أو نتيجة لتباين سعة حزمة الخدمة السيبرانية، فنقترب رقمياً من عقدة معلوماتية تفصلنا عنها مسافات بعيدة، بينما نتباعد رقمياً عن عقدة أخرى، قد تتجاور مع العقدة التي نقطنها.

لقد نجح هذا الفضاء بامتلاك هوية، وحضور انطولوجي قاهر، لم نعد قادرين على إنكاره، كما أن هذه المرتبة الوجودية قد ترسّخت، والتحمت مع نسيج أنطولوجيا الوجود الإنساني المعاصر، بعد أن نمت خيوط نسيجها، واستطالت، فتعمّقت جذورها في التربة التي تحتضن جل الخطاطات المعرفية التي توّجه مسارات فكرنا، وتقارب بين معرفتنا المجردة، بتفاصيل الواقع الملموس، والواقع الافتراضي الذي كانت ولادته نتيجة حتمية للأنطولوجيا السيبرانية المستحدثة.

2 . معمارية فضاء الفيض السيبراني:

تتألف معمارية فضاء الفيض السيبراني من مجال رقمي ـ متخيّل، يستوعب جميع الكيانات السيبرانية *IT-entities* القاطنة في بيئة الانترنيت، ويقري أنشطة الاتصال والتواصل التي تسري داخل حدود مواقعها وتطبيقاتها المتنوعة (*Floridi,2014*).

وتتكون شبكة المعلومات (التي ينتقل في قنواتها الاتصالية المتفرعة، والمتشابكة الفيض السيبراني العولمي) من مجموعة عقد اتصالية، وقنوات ارتباط، يسري فيها الفيض السيبراني الذي يسافر لتحقيق التواصل بين مختلف مراتب الكيانات التي تستوطن نسيجها الشبكاتي. وتمتلك كل عقدة معلومات عنواناً رقمياً فريداً، يميزها عن مليارات العقد التي تشكّل مادة النسيج الشبكاتي. ويسهم هذا العنوان في تنظيم مسار الفيض السيبراني من مصدره باتجاه الجهة التي يسافر نحوها الخطاب السيبراني المحمول في مادته.

وتستقر ادواتنا الاتصالية (حواسب، وهواتف ذكية، وغيرها من أدوات السيبرانية والاتصالية) عند حافات الوسط البيني، الذي يمارس أنشطته التواصلية عبر تقنيات ألياف الاتصال السلكية، أو قنوات الاتصال اللاسلكية، التي تقوم بعملية وصل المستخدمين بالنسيج الشبكاتي للانترنيت من خلال بوابات التواصل التي توفرها هذه الأدوات(*Iniewski,2010*).

ويشرف على عمليات الاتصال والتواصل (التي تسري في فضاء الفيض السيبراني) بروتوكولي *TCP/IP* لضمان سلامة سريان مادة الفيض (بواسطة بروتوكول *TCP*)، والاشراف على تطابق عنونة عقد المعلومات بين الجهة المرسلة والمتلقية (بواسطة بروتوكول *IP*).

ويوفر هذين البروتوكولين مناخاً اتصالياً آمناً، من خلال إشرافهما المستديم على كيفية تهيئة حزم البيانات، وعنونة مساراتها، ونقلها من مصادرها باتجاه غاياتها، وتحديد خارطة طريق انتقالها، والتأكد من سلامة وصول المحتوى الى الجهة المتلقية (*Wikipedia,2015*).

وتدار هذه العمليات من خلال بنية شبكاتية، تتألف معماريتها المجرّدة من أربع طبقات هي (من الأسفل الى الأعلى) :(*Bradford,2007*)

- ✓ طبقة الارتباط *Link Layer* التي تحتوي على متطلبات التواصل داخل حدود شبكة منفردة.
- ✓ طبقة الانترنيت *Internet Layer* التي تنهض بمهمة ربط المضيفات عبر شبكات معلومات مستقلّة لتؤمن عمل بيئة الانترنيت.
- ✓ طبقة النقل *Transport Layer* التي تؤمن عملية تناقل البيانات بين المضيفات المختلفة.
- ✓ طبقة التطبيقات *Application Layer* التي تنهض بمهمة تبادل البيانات.

ويلتحق بهيكلة شبكة الانترنيت مضيف *DHCP* الذي يقوم بتوزيع تفاصيل عناوين بروتوكول الانترنيت *IP*، بصورة تلقائية، إضافة الى جدران نارية *Firewalls* قد تتكوّن من عتاد رقمي، أو برمجيات لإدارة أمن الشبكة، وحمايتها من محاولات الاختراق، والتهديدات السيبرانية.

بصورة عامة، تشكّل البيانات، وخاصية الاتصالية *Connectivity*، أهم عنصرين من عناصر فضاء الفيض السيبراني. فتعد البيانات المادة الأساسية التي تشكّل جوهر الفيض السيبراني الذي يسافر جيئة وذهاباً في نسيج شبكة الانترنيت، وشبكات المعلومات التي تلتحم عقدها مع نسيجها السيبراني المعقّد. بينما تساهم الاتصالية في ربط الكيانات السيبرانية التي توطنت في فضاء الفيض السيبراني، وتغذيها بالبيانات التي تحمل مادة الخطاب السيبراني، الذي يسري في هذا الفضاء.

2 . 1 . محيط فضاء الفيض السيبراني *Infosphere*:

ليس من السهل تحديد المساحة التي ينبسط على أرجائها محيط فضاء الفيض السيبراني، وذلك بسبب الخصائص الفريدة لبيئته المتخيّلة، وعدم انصياعها للمحددات التي تفرضها خطاطة الفضاء الاقليدية على مجالات محيطنا الحيوي.

من اجل هذا سنحاول صياغة أنموذج مبسط لوصف هذا المحيط من خلال العناصر التي تسهم بتشكيل مادته السيبرانية. بداية تشكّل أدوات المعلومات والاتصالات، وعقدها الاتصالية مادة نسيج هذا المحيط، ومنافذ الولوج الى فضائه المتخيّل، الذي يمرّ بحالة نمو مستمرة نتيجة لتكاثر الأدوات السيبرانية الملتحقة بنسيجه، وازدياد عدد القاطنين في فضاء هذا المحيط.

يمكن أن نلاحظ من بيانات الجدول (1-4) أن الفضاء الاتصالي للهواتف المحمولة والذكية بات يؤلف الجزء الأكبر من حجم محيط المعلومات المعاصر (تبلغ عدد عقده الاتصالية 6.8 مليار عقدة، ويشكّل نسبة 77.5 % من العدد الكلي للنوافذ المطلّة على محيطه السيبراني). ويأتي بالمرتبة الثانية الفضاء الاتصالي الذي يتشكل عن توظيف الحواسب (المنضدية، ولمحمولة واللوحية) الذي قاربت أعدادها حوالي 1.971 مليار عقدة اتصالية بنسيج المحيط الشبكاتي، وبنسبة مشاركة تقارب 22.5 % من العدد الكلي للنوافذ المطلّة على محيط المعلومات السيبراني.

الجدول (4-1) ـ منافذ الدخول الى فضاء الفيض السيبراني العولمي ـ عام 2014.

الأداة الاتصالية	العدد	النسبة
الهواتف المحمولة.	5.2 مليار	% 59.3
الهواتف الذكية.	1.6 مليار	% 18.2
الحواسب المحمولة.	789 مليون	% 9.0
الحواسب المنضدية.	743 مليون	% 8.5
الحواسب اللوحية.	439 مليون	% 5.0

المصدر: *Meeker,2014*.

ويمكن أن يبرر تضخم الدور الذي تمارسه الهواتف المحمولة في تشكيل مادة محيط المعلومات المعاصر بسبب بساطة نظم تشغيلها، مع انخفاض أسعار هذه الأدوات الاتصالية، بالمقارنة مع أسعار الحواسب المنضدية والمحمولة، وملازمتها لأصحابها حيثما حلوا وارتحلوا، على توسيع دائرة استخدامها للدخول الى فضاء الفيض السيبراني، بحيث بدأت تشكّل تحد ياً للحواسب المحمولة، فدفعت الشركات المصنعة الى ابتكار الحواسب اللوحية بوصفها حلاً وسيطاً للاتصال والتواصل السيبراني في وقتنا الراهن.

وتشير احصائيات عام 2014 الى أن الهواتف الذكية والحواسب اللوحية أضحت تستهلك حوالي 56 % من المحتوى السيبراني القاطن في مواقع الانترنيت (44% حصة الهواتف المحمولة+12% حصة الحواسب اللوحية)، بينما تستهلك الحواسب المحمولة والمنضدية 44 % من مادة المحتوى السيبراني (*Gunelius,2014,a*).

ولا زالت عملية التحوّل نحو استخدام أجهزة الهواتف المحمولة للولوج الى فضاء الفيض السيبراني مستمرة ـ أنظر (الجدول 4-2).

الجدول (4- 2) ـ مستويات استهلاك المحتوى السيبراني في الحواسب والهواتف الذكية والحواسب اللوحية عام 2014.

فئة المحتوى السيبراني	نسبة الاستهلاك %		
	الحواسب المحمولة	الهواتف الذكية	الحواسب اللوحية
قنوات الراديو.	5	79	16
الألعاب السيبرانية.	15	79	6
شبكات التواصل الاجتماعي.	28	61	11
أحوال الطقس.	31	61	9
التسوق الالكتروني.	47	39	14
مسائل الصحة.	50	45	5
الأخبار.	55	39	6
الرياضة.	56	38	6
الغذاء والتغذية.	58	27	15
التجارة والأعمال.	62	36	2

المصدر: (*Gunelius,2014,a*).

ويبدو جلياً من هذه البيانات أن الهواتف الذكية تتفوق في كثير من المجالات على الحواسب المحمولة واللوحية، وبالخصوص عندما يتعلق الأمر بالنشاطات التواصلية اليومية، بينما لا زالت الحواسب المحمولة تتفوق في الأمور التي تتصل بأنشطة التجارة والأعمال، وأمور تتعلق بالملف الصحي والغذائي للمستخدمين، والتي تتطلب عناية ومتابعة دقيقة.

الجدول (4- 3) ـ عدد الهواتف المحمولة قبالة أعداد المستخدمين على المستوى العولمي خلال السنوات 2014-2018.

البيانات	العدد، مليون				
	2014	2015	2016	2017	2018
عدد مستخدمي الهواتف المحمولة.	5,674	5,808	5,945	6,085	6,228
عدد الهواتف المحمولة.	7,733	8,627	9,628	10,825	12,165

المصدر: *Radicati,2014*.

ويضاف الى هذا العدد الضخم، عدد أشد ضخامة يصعب احصاؤه من أدوات المعلومات والاتصالات التي تشكل الوسط البيني الذي يربط بين هذه الأدوات، مع منافذ الدخول، وارتباطها جميعاً بالعمود الفقاري لقنوات الانترنيت الاتصالية.

وكما أسلفنا، فإن هذا المحيط لا زال يمر بحالة مستديمة من القفزات النوعية، على مستوى تطور تقنيات ترابط عقده السيبرانية، وتنوّع منافذ الدخول، من جهة، وازدياد إقبال الانسان المعاصر على منصات تطبيقاته التي نجحت بترسيخ حضورها المتين في جل ميادين حياتنا اليومية ـ أنظر الجدول (4-4).

الجدول (4-4) ـ مخطط زمني للتطورات الحاصلة في فضاء الفيض السيبراني العولمي.

بيئة الانترنيت	
السنة	**الحدث**
1969	ربط أربعة حواسب ضمن مشروع *ARPANET*.
1984	أطلق على الشبكة مصطلح الانترنيت بعد أن ربط 1000 حاسب مضيف في مراكز البحوث والجامعات الأمريكية.
1998	بلغ عدد المستخدمين 50 مليون مستخدم يدعمهم 25 مليون حاسب مضيف.
2009	بلغ عدد المستخدمين 1 مليار مستخدم يدعمهم 400 مليون حاسب مضيف.
2012	بلغ عدد المستخدمين 2.1 مليار مستخدم.
2013	بلغ عدد المستخدمين 2.7 مليار مستخدم وبنسبة انتشار سكاني بلغت 47 %.
مواقع الويب	
1993	توفر 130 موقع ويب.
1996	توفر 100,000 موقع ويب.
2012	توفر 634 مليون موقع ويب.
خدمة البريد الالكتروني	
1971	أرسلت أول رسالة بريد إلكتروني.
2001	بلغ عدد رسائل البريد الالكتروني المرسلة 31 مليار رسالة يومياً.

بيئة الانترنيت	
السنة	الحدث
2008	بلغ عدد رسائل البريد الالكتروني المرسلة 170 مليار رسالة يومياً.
2012	بلغ عدد رسائل البريد الالكتروني المرسلة 297 مليار رسالة يومياً.
	شبكات التواصل الاجتماعي
2013	عدد مستخدمي منصة موقع *Facebook* حوالي مليار مستخدم، وبلغ عدد الاعجاب 2.7 مليار إعجاب يومياً. عدد مستخدمي منصة موقع *Twitter* حوالي 200 مليون مستخدم يغردون بمعدّل 175 مليون تغريدة يومياً. عدد مستخدمي منصة موقع *Google +* حوالي 135 مليون مستخدم. عدد مستخدمي منصة موقع *LinkedIn* حوالي 200 مليون مستخدم.

المصدر: *Gunelius, S., (2013, a)*.

أما قاطنين هذا المحيط السيبراني، فيمكن تقصّي أعدادهم من خلال مراجعة احصائيات عدد مستخدمي تطبيقات الانترنيت، على المستوى العولمي ـ أنظر الجدول (5-4).

الجدول (5-4) ـ أعداد مستخدمي الانترنيت في فضاء الفيض السيبراني ونسب الحضور من العدد الكلي لسكان الكرة الأرضية خلال الأعوام 1993-2015.

السنة	عدد مستخدمي الانترنيت	نسبة نمو المستخدمين	عدد السكان	نسبة النمو السكاني	نسبة الدخول من العدد الكلي للسكان
2015	3,366,261,156	15.0 %	7,259,902,243	1.02 %	46.4 %
2014	2,925,249,355	7.9 %	7,243,784,121	1.14 %	40.4 %
2013	2,712,239,573	8.0 %	7,162,119,430	1.16 %	37.9 %
2012	2,511,615,523	10.5 %	7,080,072,420	1.17 %	35.5 %
2011	2,272,463,038	11.7 %	6,997,998,760	1.18 %	32.5 %
2010	2,034,259,368	16.1 %	6,916,183,480	1.19 %	29.4 %
2009	1,752,333,178	12.2 %	6,834,721,930	1.20 %	25.6 %
2008	1,562,067,594	13.8 %	6,753,649,230	1.21 %	23.1%
2007	1,373,040,542	18.6 %	6,673,105,940	1.21 %	20.6 %
2006	1,157,500,065	12.4 %	6,593,227,980	1.21 %	17.6 %
2005	1,029,717,906	13.1 %	6,514,094,610	1.22 %	15.8 %
2004	910,060,180	16.9 %	6,435,705,600	1.22 %	1.22 %
2003	778,555,680	17.5 %	6,357,991,750	1.23 %	12.2 %
2002	662,663,600	32.4 %	6,280,853,820	1.24 %	10.6 %
2001	500,609,240	21.1 %	6,204,147,030	1.25 %	8.1 %

السنة	عدد مستخدمي الانترنيت	نسبة نمو المستخدمين	عدد السكان	نسبة النمو السكاني	نسبة الدخول من العدد الكلي للسكان
2000	413,425,190	47.2 %	6,127,700,430	1.26 %	6.7 %
1999	280,866,670	49.4 %	6,051,478,010	1.27 %	4.6 %
1998	188,023,930	55.7 %	5,975,303,660	1.30 %	3.1 %
1997	120,758,310	56.0 %	5,898,688,340	1.33 %	2.0 %
1996	77,433,860	72.7 %	5,821,016,750	1.38 %	1.3 %
1995	44,838,900	76.2 %	5,741,822,410	1.43 %	0.8 %
1994	25,454,590	79.7 %	5,661,086,350	1.47 %	0.4 %
1993	14,161,570	…	5,578,865,110	…	0.3 %

المصدر: *ITU,2016*.

لقد تزايد عدد القاطنين في هذا الفضاء من 14 مليون مستخدم في عام 1993، وبنسبة دخول بلغت 0.3 % من عدد السكان الكلي الى 413 مليون مستخدم في عام 2000، ومع نسبة دخول بلغت 6.7 %. ثم حصلت طفرة جديدة عام 2010 عندما بلغ عدد المستخدمين أكثر من 2 مليار مستخدم بقليل، وبنسبة دخول بلغت 29.4 %.

أما في عام 5201 فقد ناهزت أعداد القاطنين جاوزت 3.3 مليارات مستخدم يقيمون في المحيط السيبراني، وبنسبة دخول جاوزت 46 % ، وبمدة لبثٌ تتأرجح بين بضعة دقائق الى بضعة ساعات خلال اليوم الواحد، ومن خلال توظيف أكثر من هوية رقمية *e-Identity* خلال سياحة المستخدم بين مختلف منصات التطبيقات البرمجية.

وكما تتباين الكثافة السكانية على الخرائط التي تصف مناطق العالم المختلفة، كذلك فإن كثافة التوطن السيبراني تختلف بين منطقة وأخرى من مناطق الرقعة الجغرافية العولمية ـ أنظر الجدول (4-6).

الجدول (4-6) ـ أعداد مستخدمي الانترنيت في العالم خلال النصف الثاني من عام 2015.

المنطقة	عدد السكان	عدد مستخدمي الانترنيت		نسبة النمو 2014-2000	نسبة الدخول للانترنيت	النسبة العولمية المستخدمين
		2000	2014			
أفريقيا.	1,158,355,663	4,514,400	330,965,359	7,231.3 %	28.6 %	9.8 %
آسيا.	4,032,466,882	114,304,000	1,622,084,293	1,319.1 %	40.2 %	48.2 %
أوربا.	821,555,904	105,096,093	604,147,280	474.9 %	73.5 %	18.0 %
الشرق الأوسط.	236,137,235	3,284,800	123,172,132	3,649.8 %	52.2 %	3.7 %
أمريكا الشمالية.	357,178,284	108,096,800	313,867,363	190.4 %	87.9 %	9.3 %
أمريكا اللاتينية.	617,049,712	18,068,919	344,824,199	1808.4 %	55.9 %	10.2 %
استراليا.	37,158,563	7,620,480	27,200,530	256.9 %	73.2 %	0.8 %
العالم.	7,259,902,243	360,985,492	3,366,261,156	% 832.5	%46.4	100 %

المصدر: *Internet World Statistics, 2016*.

ويلاحظ أن نسبة النمو في أعداد الملتحقين في محيط المعلومات السيبراني لكل من أفريقيا، والشرق الأوسط، وأمريكا اللاتينية (خلال السنوات 2000-2015) قد تراوحت بين 60 الى 16 ضعفاً عما كانت عليه، بعد ان توفرت أدوات معلومات واتصالات في بلدانها، مع تدني أسعارها بحيث هرع الكثير من سكان هذه المناطق للالتحاق في فضائه المتخيَل. لكن بلدان هذه المناطق لا زالت تتراجع بشكل كبير أمام نسبة الدخول التي نلاحظها في أمريكا الشمالية وأوربا التي تجاوزت 87 %، و70 % من عدد السكان على التوالي.

2 . 2 . حجم الفيض السيبراني:

شهد حجم الفيض السيبراني (المتدفق في فضائه السيبراني ـ المتخيّل) نمواً كبيراً خلال عقدين من الزمان. ففي عام 1992 بلغ حجم الفيض الذي تدفق بفضاء الانترنيت 100 GB باليوم، وبعد عشر سنوات ارتفع حجم الفيض السيبراني الى 100 GB/sec، أما في عام 2012 فقد وصل حجم المرور السيبراني الى 12,000 GB/sec (*CISCO,2014,a*).

وإذا أردنا تقريب هذه الأرقام الى أمور أكثر قرباً من حياتنا اليومية، يمكننا القول إن حجم الفيض السيبراني المتوقع لعام 2018 سيبلغ حوالي 400 Terabits/sec والذي يكافئ بيانات أفلام فيديوية، يراقبها 148 مليون شخص، في جميع ساعات النهار، وبجميع أيام السنة. بمعنى آخر سيكافئ حجم المرور السيبراني السنوي محتوى 395 مليار قرص مدمج *DVD* (أي سيستغرق الانسان حوالي 5 ملايين سنة لمشاهدة المحتوى الفيديوي الذي سيبث داخل حدود فضاء الفيض السيبراني كل شهر من شهور عام 2018).

كذلك ستتزايد حصة المواطن من مادة الفيض السيبراني، وسترتفع من 7 GB لكل شخص شهرياً، عام 2013 الى 17 GB لكل شخص شهرياً، عام 2018، في حين لم تتجاوز هذه الحصة عام 2000 ما يعادل مادة فيض مرور معلوماتي قدره 200 MB فقط (*CISCO,2014,a*).

وسيصاحب هذا النمو الكبير في حجم المرور السيبراني العولمي، زيادة مكافئة في عدد أجهزة المعلومات والاتصالات، والتي يتوقع أن تتضاعف أعدادها بين السنوات 2013 و2018 بحيث سيمتلك كل مواطن ثلاث أدوات اتصالية يمارس بواسطتها عملية الوصول الى فضاء الفيض السيبراني (*CISCO,2014*) ـ أنظر الجدول (4-7).

الجدول (4-7) ـ حجم الفيض السيبراني العولمي وادواته السيبراني خلال السنوات 2013-2018.

المتغير	2013	2018
المرور السيبراني العولمي		
سرعة الفيض السيبراني العولمي *GBps*.	28,875	50,000
حجم الفيض السيبراني العولمي *Exabyte* شهرياً.	51.0	132.0
نسب استخدام أدوات المعلومات والاتصالات العولمية		
الهواتف المحمولة (غير الذكية).	37.6 %	16.8 %
الهواتف الذكية.	14.1 %	19.1 %
الحواسب اللوحية.	2.3 %	5.0 %
الحواسب الشخصية والمحمولة.	12.2 %	7.0 %
تواصل الأدوات الاتصالية فيما بينها *M2M*[104].	18.6 %	35.2 %

[104] . يطلق هذا الاصطلاح على عملية الاتصال والتواصل التي تتم بين أجهزة المعلومات والاتصالات السلكية Wired واللاسلكية Wireless فيما بينها للمشاركة بالمعلومات والتطبيقات.

أخرى.	5.2 %	4.1 %
نسبة الفيض السيبراني في أدوات المعلومات والاتصالات		
الهواتف المحمولة (غير الذكية).	0.1 %	0.1 %
الهواتف الذكية.	3.5 %	16.1 %
الحواسب اللوحية.	2.2 %	14.0 %
الحواسب الشخصية والمحمولة.	67.2 %	42.8 %
تواصل الأدوات الاتصالية فيما بينها *M2M*.	0.4 %	2.8 %
أخرى.	0.1 %	0.4 %

المصدر: *CISCO,2014,a*.

كما أن القدرات الاتصالية لهذه الأدوات سوف تقفز قفزات نوعية، على التوازي مع اطراد سرعة خدمة الانترنيت العريضة *Broadband* والتي ستزداد من 12 MBps عام 2013 الى 42 MBps في عام 2018.

ومن جهة أخرى، أظهرت الدراسة التي قامت بها شركة سيسكو الأمريكية المتخصصة بمجال المعلومات والاتصالات، أن فيض المعلومات العولمي سيمر بمراحل نمو متلاحقة، تبلغ نسبتها السنوية ـ التراكمية حوالي 21 %، وستتضاعف كمية الفيض السيبراني المتدفق في فضاء الانترنيت من 51,168 PB في عام 2013 الى 131,553 PB في عام 2018 (*CISCO,2014*) ـ أنظر الجدول (4-8).

الجدول (4-8) ـ نمو حجم الفيض السيبراني العولمي (وحدة *PB* شهرياً) خلال السنوات 2013-2018.

المتغير	2013	2014	2015	2016	2017	2018	النمو السنوي التراكمي
التصنيف بحسب طريقة تجهيز الخدمة							
الانترنيت الثابت.	34,952	42,119	50,504	60,540	72,557	86,409	20 %
الانترنيت المحمول.	1,480	2,582	4,337	6,981	10,788	15,838	61 %
التصنيف بحسب قطاع الاستخدام							
المستهلك.	40,905	50,375	61,439	74,361	89,689	107,958	21 %
التجارة والأعمال.	10,263	12,100	14,300	16,899	20,016	23,595	18 %
التصنيف بحسب المناطق الجغرافية							
الباسيفيك الآسيوي.	17,950	22,119	26,869	32,383	39,086	42,273	21 %
أمريكا الشمالية.	16,607	20,293	24,599	29,377	34,552	40,545	20 %
أوربا الغربية.	8,396	9,739	11,336	13,443	16,051	19,257	18 %
وسط وشرق أوربا.	3,654	4,416	5,443	6,666	8,332	10,223	23 %
أمريكا اللاتينية.	3,488	4,361	5,318	6,363	7,576	8,931	21 %
الشرق الأوسط وافريقيا.	1,074	1,546	2,174	3,027	4,108	5,324	38 %
المجموع							
المرور السيبراني.	51,168	62,476	75,739	91,260	109,705	131,553	21 %

المصدر: *CISCO,2014*.

ويتوقع أن تشكل الأنشطة الاتصالية والتواصلية للمواطن ما يقارب 4 اضعاف حجم المرور السيبراني الذي تنتجه أنشطة التجارة والأعمال. أما على الصعيد المناطقي، فتستأثر أمريكا الشمالية، والباسفيك الآسيوي بحصة الأسد من حجم المرور السيبراني العولمي.

بالمقابل، يلاحظ أن حجم المرور السيبراني في منطقة الشرق الأوسط وشمال أفريقيا سينمو بصورة سريعة، وبنسبة ستبلغ 38 % خلال السنوات 2013-2018 قبالة متوسط النمو العولمي الذي سيبلغ حوالي 21 %. وستبلغ كمية الفيض السيبراني عام 2018 بالمنطقة حوالي 5.3 Exabyte شهرياً (أي ما يعادل مادة محتوى 1 مليار قرص مدمج DVD). ويصح الأمر مع أنشطة التجارة والأعمال التي سينمو فيضها السيبراني بالمنطقة بنسبة 23 % قبالة المتوسط العولمي الذي سيقارب نسبة 18 % (*CISCO,2014*).

أما توزع مادة المرور السيبراني بين قنوات مواقع الويب، وحسابات مواقع شبكات التواصل الاجتماعي، فيمكن متابعتها من خلال بيانات الجدول (4-9)، حيث يلاحظ تفوق المرور في مواقع الويب في كل من أمريكا الشمالية، وامريكا الجنوبية، وأوربا الغربية، ووسط وشرق أوربا، ودول الشرق الأوسط، وشرق آسيا، وأستراليا على المتوسط العولمي الذي بلغت قيمته 35 %. بينما يلاحظ تراجع كل من أمريكا الوسطى، وافريقيا، وآسيا الوسطى، وجنوب شرق آسيا عن قيمة المتوسط.

الجدول (4-9) ـ المشهد العولمي لفضاء الفيض السيبراني عام 2014.

المنطقة	رواد فضاء الانترنيت		رواد شبكات التواصل الاجتماعي	
	العدد	النسبة	العدد	النسبة
أمريكا الشمالية.	284,093,742	81 %	197,033,600	66 %
أمريكا الوسطى.	66,034,487	34 %	66,951,880	34 %
أمريكا الجنوبية.	193,655,950	47 %	179,145,980	44 %
أوربا الغربية.	326,197,681	78 %	185,034,740	44 %
وسط وشرق أوربا.	174,727,847	54 %	106,440,000	33 %
الشرق الأوسط.	102,346,717	37 %	66,900,000	24 %
أفريقيا.	205,185,547	18 %	79,851,240	7 %
آسيا الوسطى.	32,444,899	29 %	5,740,000	5 %
جنوب آسيا.	188,303,759	12 %	112,696,000	7 %
شرق آسيا.	756,093,363	48 %	678,728,200	43 %
جنوب شرق آسيا.	155,173,606	25 %	161,996,000	26 %
استراليا.	23,025,488	63 %	16,163,220	44 %
العالم.	2,484,915,152	35 %	1,856,680,860	26 %

المصدر: *WAS,2014*.

اما على صعيد المرور السيبراني في قنوات شبكات التواصل الاجتماعي، فيلاحظ أن كل من: منطقة الشرق الأوسط، وافريقيا، وجنوب آسيا، قد تراجعت عن المتوسط العولمي الذي بلغت قيمته حوالي 26 %.

2. 3. جغرافية فضاء الفيض السيبراني:

لا نكاد نعثر على مفردات الجغرافية السياسية ضمن مجالات فضاء الفيض السيبراني الذي يتسم بغياب مفاهيم الجغرافية التقليدية التي تلاشت ضمن خطاطة الفضاء السيبراني المتخيّل. فالحدود التي ترسم جغرافية البلاد، وترسّخ حدودها الوطنية لم تعد حاضرة في هذا الفضاء، وبدأنا نستشعر الحاجة نحو إيجاد مفاهيم بديلة يمكن من خلالها الإمساك ببعض تلابيب الحدود الافتراضية للبلاد، في محاولة لتحديد مجالات بسط سلطة الدولة، وتحديد هوية مواطنيها الذين يقطنون الفضاء السيبراني.

لا شك أن كل دولة تشغل جزءاً معيناً ومحدداً على سطح الأرض وتتمتع بالسيادة العامة عليها. من أجل ذهب المتخصصون في عالم الجغرافية السياسية الى عد الدولة ظاهرة مساحية تستمد وجودها من أرض يقيم عليها أفراد الأمة حيث يعيشون عليها، ويمارسون فيها تفاصيل حيواتهم (العيسوي،2000).

وتتحدد حدود الدولة[105] من خلال مسطح شامل تتضح ملامحه بخطوط حدودية تميزها عما يجاورها، وتفصل أرضها عن الأراضي المجاورة لها (جاسم،2013). والتخوم سواء امتد حضورها من ظواهر طبيعية، أو لغوية، أم دينية، أم عرقية، فتتميز برسوخها وتغلغلها في الطبقات الجيولوجية العميقة لتربة الأرض التي تنتمي إليها، لذا يصعب إلغاءها أو تغييبها عن واقع الدولة بسبب انتماءها الى الماضي، مع وجود فرص لحدوث نقلات في بعض خصائصها. أما الحدود فقابلة للتغير بفعل المؤثرات السياسية التي قد تحمل آثارها على تفاصيل الجغرافية السياسية للبلاد.

إن ارتباط سيادة الدولة بالمساحة التي تمتد عليها آثار سلطاتها وهيمنتها يحتّم علينا بيان مساحتها بدقة، لتحديد مديات امتداد سلطانها. وعليه سنكون بحاجة الى تحديد حدودها التي تمتلك دلالة داخلية، ويثمر عن ترسيمها لترسيخ حدود حمى الحكومة المركزية. أما التخوم فدلالتها خارجية لأنها تحدد ملامح الجزاء الذي يقع خارج سلطاتها وهيمنتها[106]. و ما دامت الدولة تستمد مجالها من المتغير الجغرافي، فإن حضور الدولة في فضاء الفيض السيبراني يحتّم علينا تشخيص حدودها على الأرض المتخيلَة التي يقيم فيها سكانها، إذ لا وجود للدولة دونهم. كما أن وجود السكان وممارسة حيواتهم على رقعتها الجغرافية سينشئ نمطاً من العلاقة الحميمة التي ينصبغ بها مواطنو الدولة، وتتميز بها هوية الدولة عن نظيراتها (سعودي،2010).

وإذا كانت المحددات الطبيعية تعد عنصراً مضافاً للحدود الجغرافية التي تسهر الدولة على حمايتها من توغل الغير الى داخل حمى البلاد، فإن مضيفات الخدمات السيبرانية *Servers*، *Routers* تعد البوابات السيبرانية التي يسري في قنواتها الفيض السيبراني الذي يؤلف لباب مادة الحضور السيبراني في الفضاء الجغرافي المتخيّل، كما يشكّل بالوقت ذاته بوابة يمكن استغلال غياب المراقبة الأمنية عن مجالها في ممارسة عمليات التوغل الى فضاء الفيض السيبراني للبلاد.

وقد اصطنع العاملون في مجال فضاء الفيض السيبراني نظاماً فريداً لوصف وعنونة التوطن الجغرافي للموارد السيبرانية، وحضور مختلف طبقات المستخدمين في الفضاء المتخيل لبيئة الانترنيت اعتمد مبدأ تقسيم مادته الى مجموعة مركبة

---

[105]. بصورة عامة، يستخدم العاملون في ميدان الجغرافية السياسية نظامين لتصنيف الحدود الدولية، يعنى أولهما بتصنيف الدولة بحسب طبيعة العلاقة القائمة بين خط الحدود، وانتشار المظاهر الثقافية للدولة التي تفصلها عما يجاورها وتحدد ملامح هويتها الثقافية المميزة. أما الثاني فيسعى الى الربط بين الحدود الدولية والخصائص الوصفية *Morphological* سواء اصطنعها الانسان، أو طبيعية (سعودي،2010).

[106]. ورغم تقارب دلالة اصطلاحي الحدود *Boundaries*، والتخوم *Frontiers* خارج دائرة علم الجغرافية السياسية، إلا أن الخطاطة المعرفية الجغرافية قد أرست حدوداً اصطلاحية للتمييز بينهما (العيسوي،2000). فالحدود لا تنفك عن كونها إطاراً خارجياً للمساحة التي تهيمن وتدير مقاديرها الدولة، بينما تمثل التخوم مساحة للصلاحيات الحدية التي تشترك بها مع دول الجوار.

من العنونة السيبرانية. ابتكر الوصف الجديد للفضاء السيبراني على يد العالم *Paul Mockapetris* في عام 1983 وأطلق عليه اصطلاح نظام أسماء النطاقات *Domain Name System* والذي تلقفته أكثر من جهة بالتعديل، والتطوير ليكون قادراً على توفير وصف دقيق لعنونة جغرافية المواقع السيبرانية في فضاء الانترنيت (*Conrad,2000*). ويتألف نطاق التسمية[107] من ثلاثة حقول:

- الحقل الأول: فضاء الاسم *Name Space*.
- الحقل الثاني: عنونة المضيفات التي توفر فضاء الاسم.
- الحقل الثالث: عنونة الزبون (ويطلق عليه اصطلاح المحلل *Resolver*) الذي يستعلم المضيف حول فضاء الاسم ذاته.

وقد سارعت الولايات المتحدة الأمريكية الى فرض هيمنتها على هذا الفضاء بعد أن أصدر الرئيس الأمريكي السابق كلينتون قراراً الى سكرتارية التجارة في وزارة التجارة الأمريكية في صيف عام 1997 للبدء بخصخصة نظام أسماء النطاقات *DNS* لتنشيط التنافس في هذا المجال وإتاحة الفرصة أمام المساهمة العولمية في إدارة نطاقات عنونة مواقع الانترنيت. حيث هرعت وزارة التجارة الى الالتزام بالتوجيه الرئاسي فأنشأت، بالربع الأخير من عام 1998، هيئة غير ربحية للانترنيت أوكلت لها مهمة تحديد أسماء نطاقات الاستخدام في فضاء الإنترنيت، وأطلق عليها اسم *ICANN* (*Internet Corporation for Assigned Names and Numbers*). لقد أسهمت عملية تأسيس هذه المنظمة في إعطاء الولايات المتحدة فرصة الهيمنة وفرض سطوتها على تحديد وعنونة المواقع الجغرافية العولمية لفضاء الفيض السيبراني، رغم إعلانها عن حضور نظام عولمي مركزي تساهم جميع دول العالم في إدارة عملية حوكمة محتوى فضاء الانترنيت، وترسيخ قواعد الحضور فيه والانتماء إليه.

وقد تعالت أصوات دول عدة، منها الصين، وروسيا، وإيران بالاعتراض على ارتباط هذه المنظمة بالحكومة الأمريكية حصراً، مع تمتعها بصلاحيات حصرية (تعاقدية انصبغت بصبغة سياسية) في تحديد وعنونة جميع أسماء النطاقات السيبرانية *gTLDs & ccTLDs* لحضور المجتمع العولمي في فضاء الفيض السيبراني.

وتتألف البنية التحتية لنظام أسماء النطاقات من مجموعة من الكيانات السيبرانية التي تمارس عمليات الحوسبة وإدامة الاتصال بين العقد السيبرانية المتوزعة على عموم الرقعة الجغرافية العولمية. ويقوم فضاء الاسم (الذي يمثل الفضاء الكلي لجميع أسماء النطاقات) بتنظيم هذه الأسماء ضمن معمارية، تتبوأ قمة الهرم جذر النطاق *Root Domain*. أما المستوى الذي يلي هذه الطبقة فيطلق عليه اصطلاح نطاق المستوى الأعلى *Top-Level Domain* (*TLD*).

ويطلق على كل نطاق من نطاقات *TLD* التي تلي سابقتها، نطاق المستوى الثاني *Second-Level Domain*. ويتوفر بضعة مئات الألوف من أسماء النطاقات العليا، والتي تبويبها الى ثلاث فئات:

1. أسماء نطاقات المرتبة الأولى الخاصة برموز البلدان *Country-Code TLD (ccTLDs)* التي تلتحق بأسماء البلدان، وتحدد معالم هويتها على الخارطة السياسية. ويتوفر بالوقت الحالي أكثر من 240 اسم نطاق لهذه النطاقات، مثل: *ir.* الذي يؤشر الى دولة إيران.

---

[107] . تتألف البنية السيبرانية لاسم النطاق من تراتبية رمزية تبدأ بالعقدة السيبرانية وتنتهي بالجذر *Root*، حيث يفصل بين حقولها الرمز النقطي *Dot*. ويتألف فضاء الاسم من 127 مستوى، بينما يحدد طول اسم النطاق بـ 255 رمزاً. ويشكل كل اسم نطاق، نطاقاً ثانوياً *Subdomain* بالنسبة للعقدة السيبرانية التي تستوطن بالمستوى الذي يسبق مستوى توطنها السيبراني، والتي تعد لاحقة لعقدة أخرى، تشترك معها باسم النطاق ذاته.

2. أسماء نطاقات *Sponsored Generic TLDs* (*gTLDs*) والتي تحدد معالم اشتغال النشاط بمجال من المجالات التطبيقية[108].
3. أسماء نطاقات *Unsponsored Generic TLDs* (*gTLDs*) والتي تحوي نطاقات لا تدعمها مؤسسة محددة وتمثل اهتمامات ونشاطات ذات صبغة مجتمعاتية صرفة[109].

يحتل نظام أسماء النطاقات أهمية بالغة على صعيد ممارسة أنشطة الحوكمة في فضاء الانترنيت. ويثير حضور هذا النظام، وإقامته المستديمة في الولايات المتحدة، حفيظة الكثير من الدول المناهضة لسياسات الولايات المتحدة وممارساتها على صعيد الملفات الأمنية والسياسية (*DeNardis,2015*).

وتكمن هذه الأهمية في استبطان رموز هذا النظام، الكثير من تفاصيل المحتوى السيبراني الذي استودع في العقد السيبرانية، إضافة الى المعمارية المصاحبة للعنونة بحيث توفر لإدارة النظام فرصة التحكم بالكثير من تفاصيل مادته (*Sam&DeNardis,2012*).

وقد نشب عن توسع مجال تطبيقات هذا النظام في نسيج حياتنا المعاصرة، ومختلف تطبيقات المواقع التي شملت جلّ تفاصيل حيواتنا الراهنة، قد تغلغل مجسات النظام وقدرتها على تتبع التفاصيل التي لا تريد الكثير من النظم السياسية الإفصاح عن هويتها، أو معمارية توطنها في منظومتها السياسية. من أجل هذا أضحت مسألة نظام أسماء النطاقات، وحوكمة عنونة النطاقات ملتصقة بالأمن السيبراني، وهاجساً يؤرق النظم المناهضة لسياسات الولايات المتحدة، كونه يشكل ثغرة أمنية، وبوابة مفتوحة تمنح الإدارة الأمريكية فرصة ثمينة للتحكم بالفيض السيبراني العولمي، ومراقبة مادة المحتوى، والمعمارية البنيوية لموارد طبقاته المختلفة.

فعلى صعيد ملف الحوكمة السياسية تبرز الكثير من الإشكاليات، منها: هل يحق للنظام تسجيل اسم نطاق لجهة معادية لنظام من النظم السياسية، أو لجناح عسكري يمارس تهديدات مباشرة على نظام سياسي في دولة من الدول، وهل يسمح لتنظيم تعده إيران، على سبيل المثال إرهابياً، بالحصول على اسم نطاق في فضاء الانترنيت؟. وهل يحق لإدارة نظام أسماء النطاقات أن تستبعد نطاق دولة من الدولة، فتستبعد حضور مواقعها من فضاء الانترنيت، بحجة انتمائها الى مثلث الشر!.

ولا تقتصر إشكالية حضور إدارة نظام أسماء النطاقات على المسائل ذات الصلة بملفات سيادة الدول وخططاتها السياسية والتنظيمية لإدارة مشجرات عناوينها، وإنما تمتد الى مجالات ذات صلة مباشرة بمنظوماتها العقدية والقيمية. وتعد مسألة اصطناع معمارية عنونة المواقع الإباحية من الإشكاليات التي اعترضت على حضورها في معمارية النظام الكثير من الدول، منها السعودية، بينما تعاملت الولايات المتحدة الأمريكية مع هذه المسألة بوصفها فقرة من فقرات حرية المستخدم في تحديد اختياراته وميوله[110].

من أجل هذا فقد التحم رمز نطاق البلاد (*ccTLDs*) بمسائل الأمن الوطني وبدأت مؤسسات الأمن السيبراني توجه عناية مكثفة الى هرمية العنونة، والتداعيات المحتملة عن عزل جزء محدد من تفرعات شجرة العنونة الوطنية وفسح المجال أمامها لممارسة نشاطها بعيداً عن أية قيود.

---

[108] . ويستخدم لهذه النطاقات رموز محددة لتحديد هوية النشاط مثل: التعليم *edu*.، الحكومي *gov*.، العسكري *mil*.، متاحف *museum*.، وغيرها.

[109] . وتتضمن رموزاً مختلفة لوصف هذا النمط من النشاطات، مثل: تجاري *com*.، شبكاتي *net*.، منظماتي *org*.، وغيرها.

[110] . كذلك اعترضت المملكة العربية السعودية وايران على تخصيص أسماء لنطاقات تعدها مخالفة للمنظومة القيمية للدين الإسلامي، مثل: .sexy, .dating, .porn, .adult, .guy. وغيرها من أسماء النطاقات الجنسية والاباحية (*Sam&DeNardis,2012*).

ولا تقتصر التهديدات المصاحبة لنظام أسماء النطاق على هيمنة الولايات المتحدة على مقاليدها، وإنما هناك جملة من الثغرات التي يمكن استغلالها من خلال إعادة توجيه المستخدم الى مواقع مزيفة لتضليله ومنع وصوله الى الموقع المطلوب. وربما يمارس هذا النمط من التهديدات للاستيلاء على الهوية السيبرانية لمستخدم أو مؤسسة تمتلك قيمة مادية أو معنوية، أو لممارسة عمليات نصب أو احتيال، أو ممارسة عمليات الحظر على مواقع مناوئة. أما النمط الآخر من التهديدات فيشمل هجمات رفض الخدمة (*Denial of Service (DDoS*) والتي تغرق المضيف بسيل من طلبات الوصول، والقادمة من أكثر من قناة معلوماتية مما يؤدي الى شلّ نشاطه، وتعطيل الموقع عن توفير الخدمات التي يروم المستخدم الحصول عليها من صفحاته[111] (*Sam&DeNardis,2012*).

وأخيراً تبرز مسألة كشف أستار خصوصية حضور المستخدم في فضاء الانترنيت، وكشف تداعيات أفكاره من خلال احتفاظ مضيفات الخدمة بسجل تفصيلي عن عنونة المستخدم، وقائمة المواقع التي تجول في صفحاتها (*Chandramouli&Rose,2013*)، الأمر الذي يكشف عن الكثير من المسائل المهمة التي يمكن استثمارها في ممارسة تهديدات من أنماط مختلفة ترتقي من المستوى الفردي الى المستوى المجتمعاتي أو الوطني[112].

هذا ولم تعد صفة الحضور الجغرافي ـ الواقعي حاضرة في فضاء الفيض السيبراني كما هي عليه على خارطة التوطن الجغرافي التقليدي، بعد أن غيّبت جغرافية المواقع في فضاء مفتوح، تمتد حدوده بين مضيفات متعددة تستوطن أماكن متباعدة، ولا صلة لها في كثير من الأحيان بأماكن مباشرة التهديدات، والتي لا تتطابق مع التوطن الجغرافي الحقيقي. كذلك تتميز التحركات التي تصاحب التهديدات والهجمات السيبرانية ببعد زمني قصير جداً بحيث بات من الصعوبة تحديد هوية أصحابها، أو رصدها قبيل حدثها، أو اثناء ممارسة أنشطتها. يضاف الى ذلك صعوبة تمييز انتماء الجهة التي تمارس عمليات التهديد أو تباشر الهجمات على الموارد السيبرانية والمستخدمين بسبب اندماج الهويات في فضاء التعيّنات المغيبة.

وإذا كانت هوية الخصم، وموقعه الجغرافي، تعد من المسائل المهمة في إدارة النزاع ودرء المخاطر المحتملة لمنازعته، فإن انكشاف هويته وانتمائه في الفضاء الجديد باتت أمراً بالغ التعقيد نتيجة لعدم وضوح مسألة انتمائهم الى جهة محددة، أو بلد من البلدان، في فضاء مفتوح تغيب عنه ملامح الحدود الجغرافية، ولا تتضح معالم الرقعة التي يباشر منها المهاجم هجماته أو تهديداته.

3 . فضاء الفيض السيبراني: ساحة المواجهة والمنازلة الجديدة:

جلبت لنا التقنية السيبرانية فضاءً جديداً منفتحاً على ذاته، وعلى البيئات المجاورة له، بنمط غير مسبوق، ثرياً بمحتواه، يحفل بحضور طيف واسع من الكيانات، تغيب هيمنة سلطة المكان والزمان عن رقعته الجغرافية المتخيّلة، واصطنعت لنا أدواته كماً أسطورياً من البيانات التي غفل الكائن الإنساني عن تلمّس حضورها لحين أحاطت بها المتحسّسات السيبرانية، التي بدأت بالكشف عن جميع أشكال النبضات الوجودية التي باتت تطفح بها حياتنا اليومية، كنتيجة حتمية لتعدد مراتب حضورنا السيبراني في الفضاء الجديد.

غير أن هذه البنية الأنطولوجية الجديدة، لم تخل من ظاهرة توازن القوى، وتنازع السلطة على موجوداتها، شأن بقية البنيات التي لا زال الصراع عليها مستعراً بين مراكز القوى العولمية. فقد نشأ عن السلطة الغاشمة لأدوات المعلومات

---

[111] . يمكن تقسيم التهديدات المحتملة على مضيفات نظام أسماء النطاقات الى: تهديدات منصات التطبيقات البرمجية *Host Platform Threats*، وتهديدات تطبيقات نظام أسماء النطاق *DNS Software Threats*، وتهديدات المحتوى السيبراني لنظام أسماء النطاقات *DNS Data Contents Threats* وتهديدات استعلامات نظام أسماء النطاقات *DNS Query Threats*.

[112] . علماً أن هذه المعلومات يحتفظ بها دون ممارسة أي عملية تشفير مما يجعلها لقمة سائغة لأي جهة تروم ممارسة التهديدات.

والاتصالات، وتوسع هيمنة شبكة الانترنيت، والانتشار الكبير لمواقعها وتطبيقاتها على مساحة واسعة من نطاق حياتنا المعاصرة، وتراكم كم هائل من البيانات، والكيانات المعرفية السيبرانية، بروز موارد سلطوية من نمط جديد، تجاوزت مفاهيم وموجودات الاقتصاد التقليدي باتجاه اقتصاد يترعرع في البيئة الشبكاتية، ويحقق قيمته الاقتصادية المضافة من موجودات غير ملموسة، تميزت بمحتوى معرفي استمد قيمته من سلسلة المعالجات المستديمة على مادة البيانات الخام، والمعلومات (*Castells,2010*).

لقد فرضت التغييرات الجديدة التي جاءت بها خطاطة مجتمع المعلومات والمعرفة المعاصر مقولات جديدة لتحديد موارد القوة والهيمنة لدى الدول المعاصرة، فأضحت الدول الأقوى هي تلك التي تمتلك كماً أكبر من الموارد السيبرانية، وتقتني أدوات قادرة على اعتصار المادة المعرفية التي تكمن في هذه الموارد، ويلتحف مجتمعها بنسيج شبكاتي، يمتلك كفاية تقنية وأمنية رصينة (الرزو،2012).

بالمقابل تر اجعت بعض المجتمعات التي لم تمتلك نسيجاً شبكاتياً يغطي احتياجاتها، أو احتوى نسيجها على ثغرات، وفجوات أمنية يمكن أن يتسلّل من خلالها الخصم الى لباب نسيجها، فيورثه خللاً في الأداء، أو يفكّك عقده السيبرانية، فيحبط عمله، فيوقف دوران عجلة الحياة التي التحم نسيجها بنسيج الشبكات السيبرانية. في حين كتب على مجتمعات أخرى بالإقصاء وغيّب حضورها نتيجة لتراجع بنيتها التحتية للمعلومات والاتصالات عن الحدود الدنيا لمعايير الانتماء للمجتمع الشبكاتي، بحيث لم نعد نلحظ لها حضوراً على خارطة العالم السيبراني الجديدة، أو موطناً لبياناتها على قائمة البيانات التي تحفل بها التقارير والدراسات العولمية[113].

تولد عن الحضور القاهر للتقنية السيبرانية الجديدة مخاطر من نمط جديد، وبشّرت بولادة ساحة نزاع، ومواجهة، تحفل بالتهديدات، وتسري في فضائها هجمات لم نألف حضورها في عقود خلت، فتصاعدت النذر من عواقب تهديد جديد أطلق عليه اصطلاح حروب المعلومات *Cyberwar*.

لم يأت هذا المصطلح عبثاً، فقد تصاعدت الهجمات التي باشرها قاطنو العقد السيبرانية في الفضاء المفتوح للانترنيت، وتحوّلت ممارسات اللهو، وإثبات البراعة في مباشرة عملية اختراق لثغرة معلوماتية كامنة في إحدى الزوايا المظلمة من نظم المعلومات، وسخّرت لتحقيق مكاسب مادية، أو ضغوط سياسية. ثم تطورت شيئاً فشيئاً مع توسع الدائرة الإحاطية للنسيج الشبكاتي، والتطور السريع في قدرات وذكاء أدوات المعلومات والاتصالات الى تهديد حقيقي يرقى الى تهديد كيان مؤسساتي، أو مجتمع بأكمله.

فهرعت الدول الكبرى الى ترسيخ رصانة نسيجها الشبكاتي، وتسليح مؤسساتها المدنية والعسكرية بقدرات ومهارات معلوماتية تضمن سلطتها وسطوتها السيبرانية قبالة التهديدات والهجمات الجديدة. وبدأت بالوقت ذاته محاولات جديدة لتشكيل ساحة المواجهة السيبرانية *Cyber Battlefield* لكي يتسنى لها فرصة تحديد ملامح الساحة المتخيّلة للمواجهات والنزاعات الجديدة، وتكاثرت مصطلحات المواجهة الجديدة، فبرزت اصطلاحات مثل: فضاء المواجهة السيبرانية *Cyber Battle Space*، والهجمات السيبرانية *Cyber Attacks*، والتلصص السيبراني *Cyber Espionage*، والقرصنة السيبرانية *Cyber Hacktivism*، وغيرها من المصطلحات التي حوّلت دائرة النزاع، تدريجياً، من ساحة المواجهة التقليدية، الى ساحة فضاء الفيض السيبراني، حيث المواجهة اللينة بين مراكز القوى الجديدة *Soft Power*.

113 . يمكن ملاحظة غياب دول عربية مثل: سورية، والعراق، والسودان، واليمن، وليبيا عن ساحة التقارير التي تعنى بمجتمع المعلومات والمعرفة المعاصر، أو يدرج في حقولها بيانات لا تتناسب مع الواقع بسبب تراجع البنية التحتية للمعلومات والاتصالات فيها بسبب النزاعات السياسية التي تعصف بها، وعدم بلوغها مرحلة استقرار تدعم حضورها السيبراني في العالم الجديد.

3 . 1 . العمق الاستراتيجي للبيانات *Data*:

ما انفك الجنس البشري ينتج كماً هائلاً من البيانات التي تصف وتوثّق مختلف أشكال حضوره الوجودي على رقعة البسيطة. وقد ابتكر الانسان، أدوات، وآليات لإنتاج البيانات، وتدوينها. ثم توجه الى اقتراح أساليب لتصنيفها، وتبويبها، بعدما تكاثرت مادتها، وتنوّعت مصادرها، ثم اضطر أخيراً الى التوجه نحو ابتكار معالجات جديدة لاعتصارها، واستخلاص لبابها، بعد أن تصاعدت عمليات إنتاج البيانات، والمعلومات في عصر توجّه نشاطه الاقتصادي نحو التنقير عن مصادر القيمة التي تضيفها سلسلة المعالجات، التي تمارس على مادة البيانات، ولباب موارد المعلومات.

وإذا ارتبط مفهوم البيانات لدينا، منذ عقود خلت، بتدوين المشاهدات، والقياسات التي نحصل عليها من مراقبتنا لظواهر طبيعية، أو أخرى مصطنعة في مختبراتنا، أو لأنشطة اجتماعية محددة، نروم سبر خصائصها بنماذج رياضية، وأخرى منطقية، لتلبية حاجاتنا لفهم أعمق أو إعداد أنموذج وضعي للتعامل معها، فإن الأدوات التي اصطنعتها تقنيات المعلومات والاتصالات قد زودتنا بعتبة فائقة للتحسس بمستويات عميقة من التغيرات التي تسري في تفاصيل حياتنا اليومية، وبالكشف عن مختلف نزعات التغير التي تسري في محيطنا الحيوي ومحيطنا السيبراني، فوفرت لنا كماً ،غير مسبوق، من البيانات، والتي تجاوزت سعة مجالها، وتعدد ميادينها، قدرة أدواتنا على استقصاء جميع تفاصيلها، وسبر دلالاتها، وتتبع النزعات السائدة فيها، دون استخدام تقنيات مستحدثة تجاوزت عتبة العلوم الإحصائية والرياضية التقليدية، باتجاه تقنيات التنقير والسبر في مادة البيانات والمعلومات، وغيرها من تقنيات حوسبة النسيج المعقد للبيانات وكشف مظاهر التشويش والاختلاط نتيجة لتداخل الكثير من المؤثرات على عملية إنتاج مادة البيانات والمعلومات التي نجحت تقنياتنا الجديدة باقتناصها من سيل النبضات السيبرانية التي يحفل بها فضاؤنا المعرفي المعاصر.

ويتسم السريان السيبراني في فضاء الفيض السيبراني بسعات غير مسبوقة على صعيد أي نشاط مورس أو يمارس تحت قبة المحيط الحيوي للوجود الإنساني (*Floridi,2014*). وتتوالى عمليات السريان (بمختلف القنوات التي تمتلكها منصات التطبيقات القاطنة في بيئة الانترنيت) لتحمل معها كماً غاشماً من البيانات التي تستمد آنياً من مواردها، وبصورة مستديمة ـ أنظر الجدول (4-10).

الجدول (4-10) ـ حجم دفقات الفيض السيبراني العولمي[114] خلال العامين 2013،2015.

مادة الفيض	حجم الفيض السيبراني PB شهرياً	
	2013	2015
المشاركة بالملفات.	6000	14000
ملفات فيديوية.	8000	34000
بريد وبيانات الويب.	3000	9000
مهاتفة فيديوية.	400	2000
ألعاب.	100	500
مهاتفة صوتية.	200	1000

المصدر: *Gunelius, S., (2014,b)*.

[114] . تقاس كمية الفيض السيبراني بوحدة 1Giga Byte=1000 MB، 1Tera Byte=1000 GB، 1 Peta Byte=1000 TB، 1Exa Byte=1000 PB، 1Zetta Byte=1000 EB . ولكي نقارب بفهمنا لهذه الوحدات الغاشمة فإن 1EB تعادل فيلم فيديو (بجودة فائقة) يستغرق عرضه 36000 سنة (*Arthur,2014*).

فخلال كل دقيقة (*Doherty,2012*):

- ✓ يتقاسم رواد موقع *Facebook* حوالي 2.5 مليون وحدة محتوى رقمي تستودع في مادة مشاركاتهم وتعليقاتهم.
- ✓ ويعمد روّاد موقع *Twitter* الى إعادة تغريد محتوى التغريدات لأكثر من 300 ألف مرة.
- ✓ ويرسل رواد موقع *Instagram* حوالي 220 ألف صورة.
- ✓ ويرفع رواد موقع *YouTube* ما يعادل 72 ساعة فيديو.
- ✓ ويبلغ عدد رسائل البريد الالكتروني حوالي 200 مليون رسالة.
- ✓ ويعالج موقع *Google* من البيانات التي تودع في مواقع الويب ما يعادل 18.3 TB، وهي تكافئ نصف كمية البيانات التي أنتجها الجنس البشري من البيانات (وبجميع اللغات الإنسانية) منذ بداية الخليقة.

إن الكم الهائل من البيانات التي ينتجها الانسان، ويوظف مختلف أدوات المعلومات والاتصالات لاقتناصها من النبضات السيبرانية التي تسري في مختلف مراتب الأنشطة التي تسود محيطنا الحيوي، وتلك التي نجح بتخزينها، وأرشفتها، بصورة يومية قد قاربت كميتها عام 2013 حوالي 5 *Exabyte*، وهي الكمية ذاتها من البيانات التي أنتجتها البشرية منذ بداية الخليقة حتى عام 2003.

لقد بلغ مقدار الفيض السيبراني الذي تنتجه ادواتنا الاتصالية والسيبرانية الجديدة، وما نضخه من مادة هذا الفيض الى فضاء الفيض السيبراني مرتبة باتت تجبرنا على ابتكار وحدات قياس جديدة، لم يعد العقل البشري قادراً على مواكبة دلالاتها في العالم الفيزيائي التقليدي، فبدانا نصورها بأمثلة تقارب فيما بينها وبين كميات يجمع بينها حشد هائل من المضاعفات العشرية غير المسبوقة حتى في علم الفلك وسعات أفلاك كواكبه العملاقة.

3 . 2 . حظوة الانتماء الى النسيج الشبكاتي *Connectivity*:

لم يعد لحضور الحواسب معنى دون ترسيخ انتمائها الى نسيج شبكاتي، يضم عدداً من الحواسب التي تتواصل فيما بينها بواسطة قناة اتصال رقمي.

وفي الوقت ذاته، أسهمت النقلة المفاهيمية التي نشأت عن الحضور الغاشم لأدوات المعلومات والاتصالات في توليد مجموعة متنوعة من فضاءات معلوماتية نجحت بجذب الانسان المعاصر نحو مجالها، نتيجة للالتقاء والتلاقح الحميم بين الموارد السيبرانية، والأدوات السيبرانية التي تتصل بها، وتتواصل معها.

فقد نجحت الخطاطة السيبرانية على بلوغ مستوى كبير من التوافق بين الأدوات السيبرانية (البرمجيات، والخوارزميات، وقواعد البيانات، وبروتوكولات تدفق البيانات، وهيكلة قنوات الاتصالات، ...) وبين الموارد الخصبة التي تستودع في البيانات الخام (*Floridi,2014*). بمعنى آخر، لم يعد هناك ثمة برزخ يحجز بين الكيانات السيبرانية التي يكتظ بها فضاء الفيض السيبراني، من جهة، وأدوات المعالجة السيبرانية التي تعتصر مادتها لإنتاج المعاني، وسبر النزعات المفاهيمية القاطنة فيها.

وبدأت جميع تفاصيل حياتنا، ونبضات وجودنا بالانتقال الى محيط المعلومات *Infosphere* الذي توسّع تدريجياً وبات ينافس المحتوى الحيوي *Biosphere* بتعدد أشكال الكيانات السيبرانية القاطنة فيه *I-entities*، وما تتميز به من خصائص فريدة، وتكاثر التفاعلات نتيجة التواصل المستديم فيما بينها، والعمليات التي تعالج مادتها، وتعقّد شبكة حضورها الأنطولوجي.

من أجل هذا لم يعد بإمكان الانسان المعاصر تصور وجود فرصة لإدارة عجلة نشاطه دون حضور قاهر للبيانات، ووفرة أدوات لإدارة مواردها، ومعالجتها لإنتاج معان جديدة نسترشد بمضامينها في إدامة حركة عجلة حياتنا اليومية. تنشأ عن عملية الالتحاق بالنسيج الشبكاتي للعقد السيبرانية، وربطها سوية بشبكة متشعبة من قنوات تناقل البيانات، والمشاركة في مضامينها، *"Connect The Dots"*، قيمة مضافة على المستويات الاقتصادية، والاجتماعية، والمعرفية، مما يجعل من مادة النسيج هدفاً ثميناً تشد انظار الخصوم إليه، بنفس الطريقة التي تشدّ إليه أنظار أنصار بيئته (*Bergman,2014*).

وكلما تكاثرت أعداد العقد السيبرانية، وتوطدت الخيوط الرابطة بين مادة نسيجها السيبراني، كلما شكّلت مناخاً مناسباً لسريان فيض أكبر من المعلومات، مع ميل أفرادها الى إلحاق المزيد من الموارد السيبرانية والمعرفية في مستودعاتها، والسعي نحو المشاركة والتقاسم بمادة المحتوى المودع في فيضها السيبراني. الأمر الذي يؤدي الى زيادة قيمة فضائه السيبراني، فيزيد من فرصة تعرضه الى التهديدات والهجمات السيبرانية بقصد استراق عنصر أو مجموعة عناصر القيمة المضافة، أو خلخلة المحتوى لأسباب تتعلق بالتنافس، والتنازع بمختلف صوره.

من أجل هذا احتلت ظاهرة الانتماء للنسيج الشبكاتي أهمية بالغة ضمن مفردات الخطاطة المعرفية التي تعنى بتقييم مستوى التهديدات السيبرانية المحتملة، في ضوء تحديد مستوى القيمة المترتبة عن الانتماء لنسيج شبكات المعلومات، بدءاً بالشبكات المحلية، ووصولاً الى شبكة الانترنيت العولمية.

وبصرف النظر عن النهج المعتمد في تحديد القيمة التي يمكن أن تتحقق نتيجة انتماء مختلف أشكال الكيانات السيبرانية، الى شبكة من شبكات المعلومات، فإن مسألة الارتباطية أضحت تشكل عاملاً مهماً لتحديد عنصر القيمة المضافة الى فضاء الفيض السيبراني، وباتت محط أنظار من يقيمون داخل النسيج الشبكاتي وخارجه، بوصفها مؤشراً ينبغي اعتباره في التعامل على صعيد النهوض، أو عند السعي لإحداث خلل أو تشويش لدى الخصم، مهما كانت أسباب الخصومة أو النزاع.

3 . 3 . جوهر فضاء الفيض السيبراني وانعكاسات خصائصه على ساحة المنازلة الجديدة:

يتميز فضاء الفيض السيبراني بكونه مجالاً فريداً، يمارس حضوراً مقارناً لفضاء العالم الفيزيائي، دون أن يندمج، أو يلتحم مع عناصره. بالمقابل تعد الأجزاء الفيزيائية، التي تشمل: العقد السيبرانية، وأدوات المعلومات والاتصالات، ومضيفات الخدمة، ومادة النسيج الشبكاتي مدخلات الى الفضاء المتخيّل، والقناة السيبرانية الفائقة *Information Super Highway* التي يسري من خلالها فيضه السيبراني، فنتمثل من خلال بواباتها الجزء الأنطولوجي من حضورنا فيه.

ولا تمتد سلطة المؤسسة الحكومية، في جل بلدان العالم، إلا الى جزء يسير من مساحة النسيج الشبكاتي لفضاء الفيض السيبراني، بينما تتقاسم الجزء الأكبر من مادة هذا النسيج شركات القطاع الخاص، وأفراد المستخدمين المنتشرين على عموم رقعته السيبرانية.

وتنهض الشركات المضيفة للخدمة السيبرانية بمسائل الخصوصية، وأمن معلومات هذا الفضاء، مع احتكار المؤسسات الحكومية التقليدية، والأمنية مسألة خصوصية موجوداتها السيبرانية، والحصانة الأمنية لخوادمها، وقواعد بياناتها، وفق سياسة ترتبط بالخطاطة الأمنية التي قد أرست مبادئها لتحقيق المستوى الذي تروم تحقيقه من الكفاية الأمنية لنسيجها الشبكاتي.

ويتبين من مراجعة السجل التاريخي للتهديدات والهجمات السيبرانية، أن بداياتها كانت موجهة نحو مادة فضاء الفيض السيبراني، سواء عن طريق كف النظم والتطبيقات البرمجية عن ممارسة دورها في اصطناع أجزاء من الفضاء

المتخيّل، أو تشويه بعض مظاهر تمثله لدينا، أو إعاقة سريان فيضه بحيث تتراجع عجلة صيرورته، فيتباطأ حضوره في هذا النطاق أو ذاك.

اما عندما تكاملت دائرة حضور الفضاء المتخيّل، وتوسعت الأرضية التي انبسطت عليها بنيته التحتية السيبرانية، وازدادت أعداد أدواته السيبرانية والاتصالية، وحققت انتشاراً في جميع مفاصل حياتنا المعاصرة، اتجهت أنظار قراصنة المعلومات والجهات التي تمارس التهديدات والحروب السيبرانية نحو العمود الفقاري الفيزيائي الذي يصطنع الفضاء المتخيل، والى عناصر أخرى من البنى التحتية لضمان إحداث تأثيرات ضارة لا تقتصر على تشويه الجزء المتخيّل من مادته، وإنما تسعى نحو اصطناع فضاء موازي يسوده التشويش، وتتخلله فوضى تسهم في إيقاف عجلة نشاط الكثير من مفاصل مجتمع المعلومات والمعرفة، أو تدخل آلتنا الاقتصادية، وآلة صناعة قراراتنا في متاهات، تفقدها توازنها، وتحبط أنشطتها.

4 . خطاطة التهديدات والحروب السيبرانية:

تعد خطاطة الحروب السيبرانية[115] النقلة الخامسة على صعيد تاريخ النزاعات والحروب التي شهدتها الإنسانية منذ بزوغ الوجود البشري على الكرة الأرضية، بعد الحروب البرّية، فالحروب البحرية، فالحروب التي مورست في الجو، ثم الحروب الفضائية التي تتنافس بالحضور على ساحتها كل من الولايات المتحدة الأمريكية، وروسيا، والصين، وفرنسا، خلال العقود الأخيرة، بعد ان تحولت المواجهات الى فضاء متخيّل، تتألف مادته من نسيج معقد من الحواسب والعقد الاتصالية المترابطة فيما بينها، وتسري التهديدات في خضم تدفق مستمر من النبضات السيبرانية التي تسافر في مختلف أشكال قنواته الاتصالية (*Shreier,2015*).

لقد تغيرت معالم البيئة الحاضنة للنزاعات والمواجهات المعاصرة، بعد أن استوطن جزء لا بأس به من أنشطتها ضمن فضاء الفيض السيبراني، وبدأت خطاطة الحروب المعاصرة التي صاغ الإطار العام لها *Clausewitz* [116]تتعرض الى سلسلة من عمليات المراجعة، وإعادة صياغة مضامين الكثير من مبادئها العامة.

وقد أوجز *Luciano Floridi* هذه المراجعات بأربع مسائل جوهرية (*Floridi,2014*):

- ✓ وفق مبادئ العمليات العسكرية التقليدية، أسهمت تقنيات المعلومات والاتصالات بإحداث طفرة تقنية غير مسبوقة على صعيد الاتصالات، والسيطرة، بحيث وفرت مناخاً مفتوحاً لاحتواء طيف واسع من العمليات المبتكرة التي أصبحت أشد تأثيراً على مستوى إصابة الأهداف، وتعميق مستويات التأثيرات المدمرة في البنى التحتية لدى الخصم.
- ✓ أتاحت القدرات الغاشمة لأدوات المعلومات والاتصالات فرصة ثمينة لجمع، وتحليل كم هائل من البيانات الميدانية لساحة المواجهة، بحيث أصبحت عملية صناعة القرارات آنية ومحوسبة بواسطة تقنيات الذكاء الاصطناعي. لقد تحولت أدوات المعلومات والاتصالات وبياناتها العملاقة الى نمط جديد من الأسلحة المؤثرة في الحروب المعاصرة.

---

[2] . يتوهم البعض فيعد الحرب السيبرانية *Cyber Warfare* حقلاً من الحقول التي تنتمي الى ميدان حروب المعلومات *Information Operations* وهو أمر لا يتوافق مع الخطاطة الجديدة التي استنبتت في فضاء الفيض السيبراني. فحروب المعلومات تتألف من جملة فعاليات وأنشطة تروم توفير البيانات التفصيلية عن الخصم، بحيث تضمن التفوق عليه. أما الحروب السيبرانية فتستخدم أدوات المعلومات والاتصالات، مسخرة فضاء الفيض السيبراني لبلوغ أهدافها، وإحداث خلل في شبكات المعلومات، وادواتها، ومنظومات البنى التحتية التي تستثمر القدرات الكبيرة لالفضاء السيبراني في تطوير أدائها، وتوسيع دائرة أنشطتها.

[116] . يعد كتاب *On War* للكاتب الألماني *Carl Von Clausewitz* (1780-1831) من أهم الكتب التي عالجت تفاصيل الحروب التي عصفت ولا زالت تعصف بالوجود البشري. ورغم أن هذا الكتاب من نتاجات القرن التاسع عشر، إلا أنه لا زال يشكل مورداً مهماً لمناقشة خطاطة الحروب في عصرنا الراهن.

- ✓ ازداد حضور أدوات المعلومات والاتصالات السيبرانية، ومجساتها السيبرانية التي تدعمها أدوات اتصالية مثل الأقمار الاصطناعية، وتقنيات التحديد العولمي للمواقع *GPS*، والحواسب العملاقة، وأضحت جزءاً لا يتجزأ من أدوات المواجهة والحروب المعاصرة.
- ✓ نشب عن تعميق الدور الذي باتت تمارسه أدوات المعلومات والاتصالات، ومواردها السيبرانية (قواعد البيانات، والبيانات العملاقة، ومضيفات الخدمات السيبرانية، ومنصات تطبيقات الحوسبة الذكية) فقرة مهمة من قائمة الأهداف التي باتت تعرض الى هجمات معلوماتية شرسة بقصد إحداث خلل أو تخريب كلي في موارد بياناتها، أو كف مضيفات الخدمات المعلومات عن عملها، أو ممارسة عملية القرصنة السيبرانية على منصات تطبيقاتها الذكية لتشويش أداء الآلة العسكرية، أو اصابتها بخلل مؤقت أو جزئي لضمان حسم المواجهات وكسب المعركة.

4 . 1 . السمات المميزة للتهديدات والحروب السيبرانية:

أسهمت البيئة السيبرانية المتخيّلة لفضاء الفيض السيبراني بدور جوهري في تشكيل السمات الفريدة، والمميزة للتهديدات والحروب السيبرانية التي تنشأ في مجالها، وتستهدف مواردها وادواتها، وتتسلل بهدوء من خلال الفجوات السيبرانية الى كياناتها وأنظمتها المنتشرة على عموم مساحة أنشطة مجتمعاتنا المعاصرة.

ويمكن إجمال أهم الميزات الفريدة للتهديدات والحروب السيبرانية بما يلي (*Songip, et.,al.,2013*):

- ✓ تتسم بشمولية وحضور كلي غير مسبوق نتيجة لتعدد أشكال الموارد والموجودات السيبرانية، وتنوّع اماكن توطنها، وتباين قيمتها الاقتصادية المضافة، وتعدد هويات الجهات التي تمتلكها، وتعدد الحقول المعرفية التي تنتمي إليها، الأمر الذي يسهم في تعقيد المجال الذي تمتد على مساحته تأثيراتها المؤذية والتخريبية.
- ✓ غياب الشخصية المميزة *Anonymous* وضياع معالم بصمة الحضور عن مشهد ساحة التهديدات والهجمات السيبرانية بالنسبة للكيانات أو المجاميع التي تمارسها، وذلك بالتخفي وراء كواليس الحضور السيبراني المموّه في فضاء الفيض المتخيّل.
- ✓ صعوبة التحكم بمسارات التهديدات، أو الهجمات المحتملة، نتيجة لغياب البعد المكاني عن فضاء الفيض السيبراني، وانفتاحه على نسيج بالغ التعقيد من شبكات المعلومات المترابطة، الأمر الذي يجعل من فرصة كف موارد التهديدات، او الهجمات السيبرانية مسألة بالغة الصعوبة لتكاثر الفرص والاحتمالات المطروحة قبالة فرص انطلاقها تجاه أي هدف، ومن أي عقدة معلوماتية قاطنة في النسيج الشبكاتي العولمي.
- ✓ نشأ عن تعقد نسيج بيئة فضاء الفيض السيبراني، وتنوّع البيئات البرمجية، ومنصات التطبيقات، وتكاثر أنواع معدات المعلومات والاتصالات، وآلية تواصلها السيبراني فيما بينها، وتحت سقف الفضاء السيبراني المفتوح، بروز ظاهرة تعدد الثغرات السيبرانية، وتنوّعها، بحيث تعمّقت سمة تراجع الحصانة الأمنية، وارتفاع عتبة عرضتها للتهديدات والهجمات السيبرانية *Vulnerability*. وقد تعمّق تأثير هذه السمة، وتزايد حجم تعرض الفضاء السيبراني الى التهديدات والهجمات السيبرانية، نتيجة للتطورات المتلاحقة في بنية أدوات المعلومات والاتصالات، وولادة الكثير من البيئات البرمجية الجديدة، أو حصول تطورات مستمرة بالبيئات البرمجية القائمة، فتفاقمت الثغرات، ونشب عن تداخل هذه العوامل، استمرار ظهور فجوات جديدة يمكن التسلل من خلالها وإحداث تأثيرات ضارة، دون أن ينتبه لوجودها مطوري الأدوات او المنصات البرمجية الجديدة.

- ✓ لا تتطلب عملية المشاركة بتهديدات أو هجمات معلوماتية كلف مالية كبيرة، أو تحضيرات ودعم لوجستي كالتي تستلزمها العمليات الحربية التقليدية، ويمكن ممارسة أنشطة الحروب السيبرانية عبر حاسب منفرد، أو مجموعة من الحواسب، مرتبطة بفضاء الانترنيت، مع توفر بعض التطبيقات البرمجية التي يوفر الكثير منها بالمجان على مواقع الويب.
- ✓ توفر للجهات التي تقوم بها فرصة تحقيق غايات سياسية وأهداف استراتيجية دون الدخول في نزاع معلن، أو مجابهة مسلّحة مع الخصم.
- ✓ إمكانية بلوغ النظم المتحكمة بتشغيل وإدارة البنى التحتية للطاقة، والاتصالات، وشبكات تزويد الطاقة الكهربائية، وقواعد بيانات منظومات الآلة العسكرية، وخلخلة أداء أسواق الأوراق المالية قبل ممارسة الفعاليات العسكرية في ميادين المواجهة والمدافعة التقليدية.
- ✓ سرعة تنفيذ التهديديات والهجمات السيبرانية التي يسافر فيضها السيبراني عبر شبكات المعلومات العريضة، ودون إنذار مسبق، الأمر الذي يورث الخصم بلبلة واسعة، مع تعاظم المخاطر التي لا تسعف صنّاع القرار باتخاذ قرارات تتوافق مع حجم المخاطر التي تنشأ عنها.

4 . 2 . مجال المواجهة في فضاء الفيض السيبراني:

لقد تحوّل فضاء وليم جيبسون من فضاء اصطنعه لمجال افتراضي أحادي الجانب الى فضاء متعدد المجالات لم يلبث أن يضم في جنباته ميداناً فسيحاً للمواجهة والمنازلة التي انصبغت بصبغة رقمية. وقد تطور هذا الميدان، واتسعت تخومه بعد أن حدثت جملة من التطورات في هيكلة عمليات التعرّض والمواجهة فأوشكت أن تقارب مرتبة المواجهات والحروب التي يحفل بها واقعنا، بحيث ألزمت المؤسسات الأمنية في كثير من الدول المتقدمة، ومؤسساتها العسكرية أن توجه اهتمامها نحو المجال الجديد، وتباشر بهيكلة مفردات حصانته وأمنه، وتوفير قوة رقمية غاشمة للذود عن حياضها الوطنية، ومقارعة المهاجمين وصد توغلهم المتخيل في فضائها السيبراني.

وقد أضفت النزاعات والمواجهات السيبرانية على فضاء الفيض السيبراني صبغة جديدة ساهمت بنقله من دائرة المحيط السيبراني، باتجاه مرتبة وجودية من نمط جديد، تتوافق مع طبيعة الأنشطة التي تنشأ عن ممارسات التدافع، والمواجهة التي باتت تنتشر بكثافة وتتعاظم مظاهر حضورها بشكل لافت. وقد اقترح اصطلاح مجال فضاء الفيض السيبراني لوصف آثار وتداعيات النزاع السيبراني وحضور ادواته داخل حدود الفضاء السيبراني المتخيَل (*Allen&Gilbert,2009*).

ويتألف فضاء المجال من مجموع العلاقات التي تربط بين الجهات التي تمارس هذه الأنشطة، وأدوات المعلومات، ونظمها التي تسخّر لتسيير دفتها، وفيض المعلومات الذي تدار دفته لتحقيق غايات هذا النمط من الممارسات، من خلال إحداث التأثيرات المرجوّة على نظم معلومات الخصم، وخلخلة أدائها، وتشويش مادتها، وبلبلة عملياتها، في محاولة للهيمنة وإحكام السيطرة على بيئته السيبرانية لتحقيق غاية محددة.

ورغم أن فضاء الفيض السيبراني يعد فضاءَ اصطنعه الانسان للانفتاح على النسيج السيبراني الذي تشكّل نتيجة عملية التواصل والاتصال بين هذه الأدوات، ومنصات تطبيقاتها المختلفة، فقد أدرج هذا الفضاء ضمن مجالات المواجهة المحتملة، شأن المواجهات القائمة في المجال الأرضي، والبحري، والجوي، ومجال حروب الفضاء الذي التحق بهم في الألفية الجديدة بعد تبني البنتاجون مبدأ حرب النجوم (*Manzo,2011*).

بالإضافة الى البيئة المتخيّلة التي يتسم بها مجال فيض الالفضاء السيبرانيي، فإنه يختلف عن بقية مجالات المواجهة والمنازعة التقليدية بحضوره المستديم والتصاقه ببقية المجالات، بحيث تستثمر الإمكانيات الفريدة التي يوفرها فضاؤه في مباشرة عمليات المواجهة بوصفه فضاءً موازياً، يوفر أدوات داعمة لسريان مختلف أنماط الأنشطة التي تفتقر إليها عمليات المنازعة والمدافعة.

ولما كان هذا الفضاء إنشاءً تقنياً ابتكره الانسان، تتألف مادته من نسيج شبكاتي، يمرّ بحالات توسع ونمو مستديمة. لذا فإن محاولة تثبيت حدود لهذا المجال، أو محاولة إلحاقه بميدان دون آخر لن يكتب لها النجاح، ذلك لأن تلاحم خيوط نسيجه، وتداخلها، وتلاحمها، يجعل من كل عقدة قاطنة في النسيج مورداً محتملاً لمباشرة هجمة معلوماتية، أو التعامل معها بوصفها هدفاً ممكناً (*Liles, et.,al.,2012*).

لقد شكّلت معمارية الفضاء السيبراني وفق معطيات الفضاء التقليدي، وشهدت ولادة فضاءات عامة *Public Spaces* يستوطن فيها جميع فئات المجتمع المعاصر (مثل شبكة الانترنيت)، بينما شيّدت داخل حدود الفضاء العام مواقع خاصة، امتلكتها حكومات، أو مؤسسات تنضوي تحت سيطرتها، أو مؤسسات وشركات من القطاع الخاص. وتكاثرت العقد السيبرانية التي تشكّل عنها امتدادات لفضاء رقمية أكثر خصوصية *Private Spaces* استوطنت في شبكات معلوماتية وبمختلف أنماط المعمارية الشبكاتية *Network Architectures*.

بصورة عامة، يترسخ حضور المستخدم (مهما كانت صفته، فرداً كان أم مجموعة، أم مؤسسة حكومية أو خاصة) من خلال التوطن في عقدة رقمية يستمد من خلالها القدرة على الحضور الآني في فضاء الفيض السيبراني المفتوح. ويتوطد الحضور من خلال استثمار خدمة تتوزع بين استخدام ملف، أو اختزانه، أو بلوغ محتوى مطروح في صفحة من صفحات الويب الموجودة في الفضاء السيبراني، أو التواصل مع الآخر بواسطة مختلف أنماط التواصل الاجتماعي التي باتت تشكّل جزءاً لا يتجزأ من حضور السيبراني للمستخدمين في فضاء التواصل الجديد (*Thornburgh,2005*).

وقد أحكم نسيج بنية تحتية اتصالية لاستضافة موارد الخدمة (سواء كانت مضيفات *Servers* أو مستودعات سحابية *Cloud Services*، وقنوات الاتصال بين العقد السيبرانية المنتشرة في النسيج الشبكاتي العولمي، والتي توظف بروتوكولات الاتصالات[117] *Communication Protocols*.

ويبدأ سيناريو هجمة فضاء الفيض السيبراني من خلال ممارسة مجموعة من المراحل التي تشمل (*Thornburgh,2005*):

- ☒ مرحلة تقصي معلومات كافية عن الهدف بدءاً بعنونة عقدته السيبرانية، وهوية البنية التحتية الاتصالية التي يستوطن فيها، والتطبيقات البرمجية التي يمارس من خلالها حضوره الشبكاتي.
- ☒ مرحلة استثمار هذه المعلومات في تحقيق عملية اختراق حمى الهدف وتحديد مستوى أهمية المستخدم، وطبيعة الخدمات والصلاحيات التي يتمتع بها المستخدم أثناء حضوره السيبراني.
- ☒ عندما تضمن عملية الاختراق للفجوة السيبرانية تباشر عملية طمر وإقحام مجسات أداة الهجمة في نسيج النظام أو كيان العقدة السيبرانية، فتسترق البيانات، أو يقحم الفايروس المحوسب، أو البرنامج الخبيث لضمان تحقيق الغاية المنشودة من الهجمة. وتتوفر بالوقت ذاته فرصة إبقاء الكيان السيبراني المطمور في نسيج النظام الشبكاتي لضمان استمرار تأثير الهجمة، أو استثمار الأداة في عمليات أخرى بالمستقبل القريب.

[117] . يعد برتوكول الانترنيت *TCP/IP* الأكثر شيوعاً في إدارة عمليات الاتصال بالفضاء السيبراني.

وتنصبغ كل عملية من هذه العمليات بسمة خاصة تنبع من النهج الذي يستخدم في تحقيق عملية الولوج الى النظام، لذا نلاحظ تنوعاً كبيراً في الأعراض، وفي التأثيرات المحتملة على النظام المخترق.

بصورة عامة تتباين التأثيرات المحتملة عن الهجمات التي تمارس على إحدى مكونات النظام السيبراني أو إحدى كياناته، من حيث شدة التأثير وشموله، والمدة الزمنية التي تستغرقها، وهوية الهدف الذي تحاول نيله، وامور أخرى تعتمد على معمارية النظام، والنهج الذي يتبناه المهاجم، وطبيعة الغاية التي يصبو الى تحقيقها من خلال هذه الهجمة، وهوية الخصم الذي دعم الكيانات التي مارست الهجمة (*DoD,2002*).

لذا تحتم على المؤسسات الحربية العولمية التهيؤ للولوج في هذا المحال المتخيَل، وتهيئة العدة، وبناء القدرات البشرية لضمان إدارة العمليات المحتمل حصولها في هذا المجال، والدفاع عن حياضه، وترسيخ الغلبة على الخصوم الذين يتوقع قيامهم بسلسلة هجمات على موارده التي ارتبطت بوشائج متينة مع البنى التحتية للمجتمع المعاصر الذي يستمد سلطته من التفوق بميدان المعلومات، وإنتاج الموارد المعرفية.

4 . 3 . السلطان أو النفوذ السيبراني *Cyber Power*:

أضحت مسألة السلطان السيبراني، والحروب السيبرانية من المسائل المهمة التي تستوطن مكانة مميزة على صعيد استراتيجيات الحروب وتوازن القوى في عصرنا الراهن، بعد ان أضحت ممارسات التنازع والمواجهة السيبرانية شائعة على صعيد القرصنة الفردية، وتهديدات فصائل المسلحين، أو على مستوى التنازع الإقليمي، أو العولمي. بيد أن ما يثير الانتباه في هذا المجال هو وجود مستويين من مستويات السلطان السيبراني، مستوى يعبّر عن حقيقة ما تمتلكه الدول والكيانات من قدرات معلوماتية تبسط سلطانها وترسخ هيمنتها، وكفاءتها قبالة التهديدات المحتملة. ومستوى آخر، يرتبط بالجهات التي تلتحق بمعسكر المواجهة والمنازعة التي قد تشتعل هنا، بعد أن خبت هناك، أو نتيجة لتحالفات أيديولوجية، وأخرى اقتصادية، أو الاعتناء بمسألة ما، أو وجود ميل نحو القضية التي تستبطن التهديد، أو الرغبة بالانتقام من خصم يستقر في معسكر الجهة المناوئة.

من اجل هذا بدأنا نلاحظ توسّع رقعة النزاع والمواجهة، وتخلل موازين النفوذ والسلطان السيبراني لهذه الجهة، أو تلك، نتيجة التحاق الكثير من أنصار القضية، مع هذا المعسكر، أو نكوصهم عن ذاك، الأمر الذي يزيد من تعقيد مسألة تحديد الدولة أو الجهة التي تمتلك السلطان الأكبر ضمن سيناريو التهديدات والمواجهات السيبرانية، ما لم نحدد بوضوح مبررات النزاع، وأرضيته، وغيرها من العوامل المتداخلة، بحيث لا يمكن تحديد رجاحة كفة على أخرى ما لم تشتعل المواجهة، وتطفو على السطح هوية الأهداف التي نالتها عمليات التهديدات والمواجهات السيبرانية.

أما الحكم المسبق الذي تعودنا إصداره على تنامي نفوذ هذه الدولة، او هذا الكيان، وذاك بناء على معلومات مسبقة، فلم تعد ذات قيمة معنوية في فضاء منفتح لجميع المستخدمين، ومتعال على الحدود الجغرافية، مع غياب هوية الجهات المشاركة، وتباين هوية الأهداف، ومستوى الأهمية الذي تشكله في فضاء لم تتضح جميع مكوناته، وقد غابت عن أنظارنا الترابطات المقيمة بين عناصره ومنصاته السيبرانية.

بصورة عامة، يذهب الكثيرون الى عد السلطان، أو النفوذ السيبراني مؤشراً على امتلاك القدرة والمهارات المناسبة لاستخدام وتوظيف الخصائص الفريدة التي يتسم بها فضاء الفيض السيبراني والكيانات والأدوات السيبرانية القاطنة أو المرتبطة بنسيجه السيبراني لضمان ميزة تنافسية، أو تحقيق مكاسب على المستويات السياسية، أو الاقتصادية، أو إحداث تأثيرات ملموسة في الفضاء السيبراني، أو الأدوات السيبرانية، أو البنى التحتية السيبرانية والاتصالية التي يمتلكها الغير متى اقتضت الحاجة لذلك.

يتولّد السلطان أو النفوذ السيبراني نتيجة انتشار أدوات المعلومات والاتصالات، وتلاحم النسيج الشبكاتي الذي يسهم في تكامل أداءها، مع توفر مهارات وخبرات معلوماتية، تمنح الجهة التي تقتنيها القدرة على استهداف، أو إحداث تأثيرات حاسمة على أهداف منتخبة من البنى التحتية للمعلومات والاتصالات، وخلخلة أدائها، وبثّ الفوضى في مواردها وقواعد بياناتها.

وتوظف الدول والجهات التي تمارس الحروب السيبرانية نفوذها السيبراني وتعاظم سلطانها المنبسط في فضاء الفيض السيبراني إما لمباشرة تهديدات رقمية، أو إلحاق أضرار كبيرة بالبنى التحتية لخصومها، أو تحقيق غايات سياسية أو اقتصادية محددة.

ويتميز النفوذ السيبراني بثلاث خصائص جوهرية:

الخاصية الأولى: الحضور الكلي والتغلغل القاهر في جميع مفاصل المواجهة مع الند.

الخاصية الثانية: تعد عملياتها جزءاً مكملاً لبقية أنماط المواجهة التي تمارس على الخصم، وذلك لمحدودية تأثيرها بالوقت الراهن وغياب صفة الشمولية عن ممارساتها.

الخاصية الثالثة: خفية على العيان، فلا يعلن عن حضور مواردها، وصعوبة تمييز هوية الجهات التي تمارس أنشطتها كونها تزاول خلسة بالتسلل بين عقد النسيج الشبكاتي العولمي، ودون إبقاء آثار التلصص على قواعد البيانات، أو نظم المعلومات. وقد تنشأ عن غرس أدوات القرصنة والتلصص السيبراني في البيئة السيبرانية لنظم معلومات، أو شبكات معلومات الخصم، فلا تباشر بممارسة أنشطتها لحين توفر شروط منطقية محددة، تحفزها باتجاه بدء التهديدات أو الهجمات التي خططت لها.

بصورة عامة، يمكننا القول أن مستوى السلطان السيبراني وعملية تشكل أركانه تتأثر الى حد كبير بجملة من العوامل. بداية يعد السلطان السيبراني مؤشراً على قدرة الموارد البشرية في توظيف بيئة فضاء الفيض السيبراني وادواته السيبرانية في ترسيخ بيئة رقمية آمنة قبالة التهديدات والهجمات المحتملة، مع توفير مستوى رصين من الحصانة والتكامل على صعيد إدارة موارد المعلومات وقواعد بياناتها، على التوازي مع تماسك عناصر البنية التحتية للمعلومات والاتصالات لتحقيق هذه الغاية.

من جهة أخرى، يلتحم مفهوم السلطان والنفوذ السيبراني بحجم البيانات والمعلومات التي نمتلكها، وتكامل مادتها، ودقة المحتوى الذي تتضمنه، ومستوى شمولها، وقدرتها على وصف الواقع بموضوعية، بحيث تمنحنا فرصة أكيدة لاستثمارها في صناعة قرارات حاسمة، وتحديد مواطن الضعف والثغرات السيبرانية القاطنة في النسيج الشبكاتي لبيئتنا السيبرانية، وبيئة الخصم ليتسنى لنا حماية مواردنا، والضغط على الخصم حينما يقرر التعرض لفضائنا السيبراني.

5. عناصر ومراحل وأدوات النزاعات والمواجهات السيبرانية:

يتميز الفضاء السيبراني بتنوّع عناصره، وامتداد نسيجه على مساحات لا يمكن حصرها بسبب انفتاحه على المكان المتخيّل الذي يقارب الخيال الإنساني في سعته وثرائه.

تسود في مجال النزاعات السيبرانية المتكاثرة في فضاء الفيض السيبراني مجموعة متنوعة من ممارسات التنازع والمدافعة، والتي قد تكلّل بنشوب نزاع شامل يرتقي الى مستوى حرب معلوماتية جامعة بين الأطراف المتنازعة. وتتدرج هذه الممارسات من محاولات تلصّص الى اختراق لنظام شبكاتي، فاستحواذ على موارد رقمية مهمة، أو تتطور باتجاه هجمة يحاول أصحابها إحداث خلل في الموارد السيبرانية أو كف النظام عن العمل بصورة جزئية أو كلية (*Libicki,2009*).

وسنحاول أن نحلل عناصر كل نشاط من هذه الأنشطة كي تتضح معالم ممارسات التنازع والمدافعة التي باتت تتكاثر بسرعة في فضاء الفيض السيبراني ـ العولمي.

بصورة عامة، تعد الثغرات الأمنية باباً مشرعاً أمام الهجمات ومختلف أضراب التهديدات السيبرانية التي تمارس على شبكات المعلومات كونها تمثل مؤشراً على مناطق الضعف وغياب الحصانة الأمنية *Vulnerability* التي تقيم بنظم المعلومات. ويمكن أن يستغل القرصان السيبراني حضور الثغرات الأمنية في التسلل الى النظم السيبرانية والكشف عن أسرارها، وبلوغ مواردها الحصينة، تمهيداً لمباشرة عمليات تخريبية (الرزو،2007).

ولا تعدو الثغرة الأمنية عن كونها خاصية تقنية يتسم بها عتاد الحاسوب أو برمجياته التطبيقية والتي يمكن أن تتيح لمستخدم غير مرخص *Unauthorized User* إمكانية اقتناص فرصة للدخول الى النظام السيبراني، أو زيادة مستوى ترخيص الدخول الى حدود غير متاحة له بدون استغلال وجود هذه الثغرة.

تنتمي الى دائرة الثغرات الأمنية مجموعة متنوعة من الخصائص والسمات التي تتصف بها مكونات النظام السيبراني، فيندرج بدائرتها أية خاصية يوفرها النظام البرمجي للمستخدم المرخّص/الشرعي (في العتاد أو البرمجيات) يمكن أن يستغل القرصان السيبراني الميزات الملحقة بها فيمتلك القدرة على الدخول الى البيئة الشبكاتية الآمنة، أو يخترق الحواجز السيبرانية ـ الأمنية التي تتحكم بمستويات الترخيص وصلاحيات أصحابها.

بصورة عامة تسود قاعدة عامة لدى العاملين في ميدان أمن المعلومات تؤكد بأنه لا يوجد ثمة موقع ضمن خطاطة البرمجيات التطبيقية، أو نسيج العقد الشبكاتية، يتمتع بكفاية أمنية تجعلها بعيداً عن التهديدات التي تمارس من خلال عمليات القرصنة السيبرانية. بمعنى آخر يمكننا القطع بغياب سمة الأمن المطلق عن أي كيان برمجي او معلوماتي في البيئة السيبرانية.

فلا يكاد يخلو أي نظام يؤسسه الكائن البشري من سمة الخطأ أو غياب سمة الكمال المطلق، كذلك فإن الثغرة الأمنية ليست خاصية منفردة تنشأ بذاتها، وإنما هي حصيلة لمجموعة من الخصائص التي ينبغي توافرها داخل حدود الشبكة السيبرانية، أو التطبيق البرمجي لضمان ديمومة عمله، بيد أن وجود هذه السمات مجتمعة في ظل هيكلة محددة يمكن أن يؤلف مقومات نشوء ثغرة، تصبح بعد حين لقمة سائغة، يمكن لقرصان ان يستثمرها في إحداث اختراق أمني.

ويمكن أن يستمر وجود الثغرة في النظام البرمجي دون أن تحدث عملية اختراق ما لم تتوفر الظروف التي يمكن أن تفصح للقراصنة السيبرانيين، أو المستخدمين الشرعيين عن وجودها نتيجة لحضور الظروف المواتية للكشف عن هويتها.

وتستثمر الجهة المهاجمة، وجود الثغرة الأمنية، في ممارسة التهديد الأمني، واختراق حمى نظام المعلومات أو احدى كياناته السيبرانية لإحداث تأثيرات سلبية على البيئة الشبكاتية، أو أحد عناصرها.

بصورة عامة هناك نوعين من التهديدات التي تستهدف البيئة السيبرانية:

النوع الأول: تهديدات غير مهيكلة *Unstructured Threats*: وتتألف عناصر هذا التهديدات من مجموعة من الأنشطة غير الاحترافية التي يمارسها بعض فئات القراصنة السيبرانيين ممن يفتقرون الى خبرة عميقة، وحنكة تقنية كافية لممارسة التهديد وفق أنموذج أعدّ بصورة مسبقة، وإنما يلجؤون الى استخدام أدوات قرصنة شائعة ذات تأثير محدود.

النوع الثاني: تهديدات مهيكلة *Structured Threats*: وتشمل طيف واسع من التهديدات التي ترتكز الى أنموذج يختص بكل حالة من حالات غياب العناصر الأمنية عن البيئة السيبرانية، ويمارسها مجموعة من القراصنة السيبرانيين

المحترفين، الذي تتضح لديهم أهداف الهجمة السيبرانية التي يمارسونها، ويمتلكون أدوات قادرة على تجاوز أي عقبة امنية في النظام لضمان تحقيق غاياتهم.

5. 1. موجز تاريخ التهديدات والهجمات السيبرانية:

لم يخلو فضاء الفيض السيبراني من التهديدات والمنازعات والهجمات رغم سمته الافتراضية المتخيّلة، وسيادة النزعة الناعمة في تطبيقاته وادواته. وقد برزت النزعات العدوانية للمرة الأولى، في هذا الفضاء، عندما حاول بعض المستخدمين الإفصاح عن قدراتهم ومهاراتهم في إحداث خلل جزئي في بعض أجزاء نسيج الشبكات السيبرانية، أو حواسيب الغير، أو التلصص على عقدة معلوماتية لدى جهة محددة للوقوف على بعض أسرارها غير المعلنة أو إشباع غريزة الفضول والرغبة في سبر موارد المجهول وغير المعلن.

لم تكن عملية التلصص، أو التسلل الى فضاء الغير، مؤذية في بدايتها، لكنها تحوّلت شيئاً فشيئاً الى مصدر للإزعاج، ولإحداث الخلل الجزئي في الحاسب، أو عموم شبكة المعلومات قبل أن تتحوّل باتجاه تأثيرات ضارة، أو مدمرة في بعض الأحيان. وقد تطورت ممارسات التهديدات والهجمات السيبرانية بعد أن ولدت تحالفات بين أكثر من جهة، نتيجة لتوافق الغايات وتطابق هوية الخصوم الاقتصادية، أو السياسية، أو الاثنية، فتطورت من ممارسات فردية الى ممارسات منسقة، وبدأت بانتخاب أهداف استراتيجية، الأمر الذي أجبر المؤسسات الأمنية والعسكرية في كثير من بلدان العالم الى التورط بممارسة هذا النشاط للدفاع عن بيضة فضائهم السيبراني، أو ممارسة النهج ذاته بمباشرة هجمات للدول والنظم التي يناصبونها العداء، أو للضغط على الخصم من خلال الهجمات السيبرانية الناعمة وغير المعلنة.

ولما كانت عملية تدوين السجل التاريخي لهذه المسألة تحتل أهمية كبيرة في سبر عناصر ومكونات التربة الحاضنة لبذرتها الأولى، مع توضيح نزعة نموها، والتطور الحاصل في الآليات المستخدمة، وتحديد هوية الأهداف المستهدفة، وسلوك الجهات التي تمارسها، فقد أولت مراكز البحوث والدراسات الاستراتيجية مساحة كافية لتتبع آثار بصماتها منذ البدايات، ولغاية وقتنا الراهن.

وقد حاولنا أن نستخلص من هذه التقارير والدراسات عصارة مفيدة تتوافق في مضامينها مع دراستنا، ثم عمدنا الى تبويب أهم مفردات هذه المادة التاريخية ضمن خطاطة توضح أنواع هذه التهديدات والهجمات، وتلك التي ارتقت الى مستوى يقارب مقدمة للحروب السيبرانية واودعناها في تسلسل زمني تدرّجت وقائعه من البدايات وحتى هذه الأيام ـ أنظر الجدول (4- 11).

الجدول (4 - 11) ـ موجز تاريخ التهديدات والهجمات ومقدمات الحروب السيبرانية.

السنة	نوع الهجمة	الجهة المستهدفة	التفاصيل
1982	اختراق معلوماتي	شركة كندية لإنتاج النط والغاز	عمدت وكالة المخابرات الأمريكية الى تنبيه الشركة الكندية حول وجود تحرك روسي لقرصنة البرنامج المستخدم في إدارة إنتاج النفط والغاز بين كندا وسيبيريا والذي قد يؤدي الى حصول انفجار في الأنبوب الناقل.

السنة	نوع الهجمة	الجهة المستهدفة	التفاصيل
1988	تسلل دودة موريس السيبرانية Morris Worm	منصة تطبيقات نظام *UNIX* في الولايات المتحدة وبقية البلدان.	تسللت الدودة السيبرانية من خلال الثغرة المستوطنة في نظام *UNIX* وباشرت بعملية التناسل المستمر بحيث تسبب عن تكاثرها توقف الحواسب المصابة عن العمل.
1990ˢ	ولادة وانتشار فايروسات الحاسب مثل: Melissa & I Love You	أصابت هذه الفايروسات وغيرها بضعة ملايين من الحواسب في عموم المجتمع السيبراني العولمي.	تسبب عن إصابة الحواسب بهذه الفايروسات وغيرها التي تكاثرت أنواعها وتعددت نزعاتها التخريبية توقف خدمة البريد الالكتروني مع تباطؤ ملحوظ في أداء الحواسب، ونجم عن بعض أنواعها المتطورة حصول خلل في عتاد الحواسب وتوقف أقراصها الصلبة كلياً عن العمل.
	استخدام برنامج الشمّام Sniffer Program في عملية تلصص واسعة النطاق	حواسب مركز تطوير القوة الجوية في قاعدة نيويورك الجوية	قامت مجموعة من قراصنة المعلومات الذين يطلقون على أنفسهم Anonymous Hackers بمهاجمة منظومة هذا المركز لأكثر من 150 مرة لسرقة شهادات الدخول الى شبكة معلومات المركز، ومعلومات مهمة من المختبرات التي تعكف على إجراء أبحاث لتطوير نظم الذكاء الصناعي ونظم التتبع الجوي. ويمكن لهذه المعلومات أن تستثمر بالدخول الى نظم حواسب وزارة الدفاع الأمريكية، ومشروع ناسا الفضائي.
2003	قرصنة معلومات حكومية	شبكات الحواسب العسكرية في الولايات المتحدة	لاحظ المتخصصون بأمن المعلومات وجود اختراقات متكررة من قبل قراصنة معلومات (يعتقد أنهم من الصين) لسرقة معلومات مهمة من شبكات حواسب وزارة الدفاع الأمريكية، من خلال استغلال ثغرات مقيمة بالنظام. وقد اطلق على هذه العملية اسم *Titan Rain* واستمرت الهجمات لمدة ثلاث سنوات.

السنة	نوع الهجمة	الجهة المستهدفة	التفاصيل
2007	هجمات معلوماتية منسقة (حرب معلوماتية مصغرة)	مواقع حكومة إستونيا	تعرضت المواقع الحكومية لإستونيا الى سلسلة من الهجمات السيبرانية (هجمات رفض الخدمة *DOS*) مما سبب توقفها بصورة كلية لمدة 22 يوماً. ويعتقد ان قراصنة معلومات روس (من المؤسسة الحكومية الروسية) قد قاموا بهذه الهجمات. وقد شملت الهجمات موقع رئيس الجمهورية، والبرلمان، والهيئات القضائية، ومؤسسات مصرفية مهمة.
	قرصنة معلومات مهمة	مواقع صينية متنوعة	أفصحت وزارة الأمن الصينية عن وجود سلسلة من هجمات القرصنة السيبرانية التي قامت بها مجاميع من الولايات المتحدة وتايوان للحصول على معلومات مهمة من قطاعات صينية مختلفة.
2008	قرصنة مواقع حكومية	شبكات المعلومات الجورجية	تعرضت مواقع الحكومة الجورجية الى هجمات قرصنة نشب عنها توقف هذه المواقع لمدة ليست بالقصيرة، أثناء الخلاف السياسي المستعر مع روسيا الاتحادية، وذلك للضغط على الإدارة الحكومية على التوازي مع العمليات العسكرية التي قامت بها القوات الروسية.
2009	قرصنة مواقع حكومية	البنية التحتية للمعلومات في إسرائيل	تعرضت البنية التحتية للمعلومات والاتصالات الإسرائيلية الى هجمات منسقة أثناء حربها مع حزب الله وهجماتها المتكررة على قطاع غزة. وقد أسفرت الهجمة عن إيقاف عمل عدد كبير من المواقع الحكومية، وقد تبين أن هناك أكثر من 5000 حاسب قد ساهم بهذا النمط من الهجمات المنسقة من خلال إغراق هذه المواقع برسائل بريد الكتروني وبمعدل 15 مليون رسالة بالثانية الواحدة. وقد اتهمت الحكومة الإسرائيلية كل من حركتي حزب الله وحماس وأنصارهما بمباشرة هذه الهجمات المنسقة.
	قرصنة مواقع حكومية	مواقع حكومية وسفارات في دول مختلفة	كشف الباحثون في مركز *Munk* بجامعة تورنتو الكندية عن وجود سلسلة من الهجمات المنسقة على مواقع حكومية وسفارات في أكثر من 103 بلداً بغرض التلصص على الموارد السيبرانية وسرقة بيانات مهمة من أكثر من 1300 حاسب مركزي.

السنة	نوع الهجمة	الجهة المستهدفة	التفاصيل
2010	قرصنة محركات بحث	محرك البحث الصيني *Baidu*	قام جيش إيران السيبراني *ICA* بمباشرة سلسلة هجمات على محرك البحث الصيني مع بث صفحة عليه حملت رسالة سياسية إيرانية.
	فايروس فتاك	المفاعلات النووية الايرانية	كشف النقاب عن السلاح السيبراني الفتاك *Stuxnet* والذي سبب خللاً كبيراً في عمل أجهزة الطرد المركزي نتيجة لاختراق نظامها البرمجي، والعبث بأجهزة البرمجة المنطقية *PLC* التي تتحكم بتشغيل مفاعلات نطنز الإيرانية.
2011	هجمات منسقة	مركز بحوث وتطوير القدرات الدفاعية ـ كندا	تعرضت كثير من المؤسسات الحكومية الكندية، وبالخصوص مركز بحوث وتطوير القدرات الدفاعية، والكثير من المؤسسات المالية الى هجمات متكررة بحيث اضطرت الى قطع ارتباطها بشبكة الانترنيت لحين تجاوز آثار هذه الهجمات.
2012	اختراق شبكة معلومات	شركة أرامكو السعودية	قامت مجموعة من القراصنة أطلقت على نفسها اسم "سيف العدالة القاطع" باختراق الجدران الأمنية لشبكة معلومات شبكة أرامكو النفطية بالسعودية وقامت بإلغاء البيانات الموجودة في الأقراص الصلبة لأكثر من 30 ألف حاسب بهذه الشركة.
2015	اختراق شبكة معلومات	البيت الأبيض ووزارة الخارجية في الولايات المتحدة	أعلنت الإدارة الأمريكية عن اكتشاف عملية اختراق قام بها مجموعة من القراصنة الروس لاختراق منصة البريد الالكتروني بالبيت الأبيض، ووزارة الخارجية مع الظفر ببيانات شخصية متنوعة لأكثر من 4 ملايين موظف بالإدارة الأمريكية.

المصدر: ***NATO,2013/ Rowen,2015***.

ينبغي الإقرار بصعوبة الإحاطة بجميع أشكال وتفاصيل التهديدات والهجمات السيبرانية في عموم فضاء الانترنيت لكثرتها وتنوع الجهات التي تمارسها، وتباين الأهداف التي تقصدها. من أجل هذا حاولنا في هذا الجدول بيان أهم الهجمات التي حدثت خلال ما يقارب الثلاثة العقود.

ذلك أن التهديدات والهجمات قد تطورت من هجمات منفردة، محدودة التأثير الى هجمات أكثر تنسيقاً ويشترك فيها أكثر من مجموعة، مع بروز آثار الصبغة السياسية على غاياتها، فقد تحوّلت الهجمات من هجمات غير موجهة الى خصم حدد، كما هو الحال عليه مع الفايروسات والديدان التي ولدت في عقد الثمانينات من القرن العشرين، الى هجمات موجهة الى مؤسسات حيوية في الدول الكبرى المتصارعة (مثل: الولايات المتحدة، والصين، وروسيا) أو بين دول منطقة الشرق الأوسط (مثلث إسرائيل وجبهات المقاومة، وحلفاء السعودية ودول الخليج وإيران) (*Otafu, et.,al.,2013*).

بالمقابل تعد ولادة فايروس *Stuxnet* الذي استهدف مفاعلات نطنز النووية تحولاً من نمط فريد في صناعة أدوات الهجمات السيبرانية التي اتسمت بتعقيد بنيتها البرمجية وتعدد أهدافها، وعدم وضوح مسارات استهدافها للمنظومات، إضافة الى تخصصها الدقيق باستهداف فئة محددة من المعدات[118].

كذلك نستطيع أن نؤكد عدم وجود آثار واضحة لما يمكن أن يعد حرباً معلوماتية وفق المعاني والدلالات الاصطلاحية بميدان الحروب العسكرية، وإنما لا تعدو هذه الوقائع عن كونها مجموعة من التهديدات، أو الهجمات المتفرقة، والتي بدأت تتسم بالتنسيق وتحديد الأهداف، وخطورة تأثيراتها، إلا انها لم ترق بأي حال من الأحوال الى مستوى الحرب بمفهومها الشائع (*NATO,2013*).

بيد أن ما حصل في إستونيا عند خلافها العميق مع روسيا، وكذلك الحال مع جورجيا يمكن أن يعد توطئة لحرب معلوماتية مصغرة يمكن أن نشهد سيناريوات مقاربة، أو أكثر تعقيداً في المجالات الساخنة في دائرة النزاع في الشرق الأوسط، أو بين الدول الكبرى في المستقبل القريب.

5. 2. الهجمة أو التعرّض السيبراني:

باتت الهجمات السيبرانية تشكل تهديداً خطيراً يقلق المؤسسات المالية والتجارية، والمؤسسات الحكومية وإداراتها العليا، بحيث أجبرت هذه التأثيرات الوخيمة الرئيس الأمريكي أوباما على الإقرار بأنها تشكل أكثر التحديات الاقتصادية والأمنية التي تهدد الشعب الأمريكي (*Rowen,2015*).

تعد الهجمة السيبرانية أو عمليّة التعرض السيبراني إحدى مؤشرات انتقال ممارسات التلصص أو الاختراق باتجاه ترسيخ نمط من أنماط النزاع السيبراني. ونظراً لانفتاح مجال فضاء الفيض السيبراني، وتعدد أنماط الممارسات التي يمكن أن يتلبس بها قطانه، وبمختلف مراتب حضورهم السيبراني، فقد تباينت الآراء حول تعريف الهجمة السيبرانية، وتأرجحت حدودها الاصطلاحية بين مستويات عدة.

وقد أثمرت تحريات أحد الباحثين (*Kadivar,2014*) وتنقيره المستمر في أوراق البحوث والدراسات التي نشرت خلال أكثر من عقدين حول هذه المسألة بالعثور على ستة تعريفات لهذا المصطلح الشائك:

1. أي نشاط يتخذ لتقويض أداء شبكات الحواسب لأغراض سياسية أو لأغراض ذات صلة بأمن المعلومات في البلاد.
2. توظيف مجموعة من الممارسات المتعمدة (خلال بعد زمني طويل) لإحداث تغيير، أو خلل، أو تشويش، أو تراجع بالأداء، أو تدمير نظم حواسب الغير، أو الشبكات، أو موارد المعلومات ومستودعاتها، أو النظم البرمجية التي تدير عملها.
3. مجموع العمليات الهجومية أو الدفاعية التي تهدف الى إحداث تغيير، أو إلغاء، أو خلخلة أو منع الوصول الى الحاسب، وموارد بياناته أو برمجياته لتنفيذ غايات تتوزع بين نشاطات: دعائية أو محاولات تشويه؛ إحداث خلل جزئي أو كلي في الحواسب أو نظمها، أو نسيجها الشبكاتي، أو بنيتها التحتية المستهدفة؛ إحداث خلل فيزيائي ـ عرضي في الحواسب أو نظمها السيبرانية، أو على مستوى نسيجها الشبكاتي.
4. استغلال فضاء الفيض السيبراني وموارده وادواته بقصد الوصول والولوج غير المشروع الى مستودعات البيانات والمعلومات المحمية، أو التلصّص والتجسس على موارد رقمية، أو إحداث شلل في أداء شبكات المعلومات ومكوناتها لغرض سرقة موارد معلوماتية مهمة أو موارد مالية ذات صلة بها.

[118] . سنتناول بنية هذا الفايروس ومسارات تأثيره على البنى التحتية للمعلومات وأداء منظومات أجهزة الطرد المركزي في الفصل القادم.

5. أي ممارسة عدوانية توظف فيها الحواسب أو عناصر نظمها السيبرانية والبنية التحتية لنسيجها الشبكاتي لإحداث ضرر أو تخريب في نظم وحواسب الخصم على مستوى المكونات، والموارد السيبرانية، أو الأداء.
6. أية جهود تبذل للوصول والولوج غير المشروع الى مستودعات البيانات والمعلومات المحمية، أو التلصّص والتجسس على موارد رقمية، أو إحداث شلل في أداء شبكات المعلومات ومكوناتها لغرض سرقة موارد معلوماتية مهمة أو موارد مالية ذات صلة بها.

إن التنقير في البعد المعرفي لهذه التعريفات يظهر لنا وجود تقارب كبير في دلالاتها الاصطلاحية بيد أن التباين يكمن في أمور تتعلق بالمجال الذي تمارس بفضائه وتتغلغل في طبقاته الجيولوجية. فالهجمة السيبرانية لا تخلو من غايات مستبطنة أو معلنة توجه مساراتها وتصبغها بصبغة تحدد هويتها (*Thornburgh,2005*).

وعلى هذا الأساس يمكن أن نعرّف الهجمة السيبرانية بكونها وصف يطلق على ممارسة توظف أدوات فضاء الفيض السيبراني ومجاله الافتراضي بوصفها عدّة، أو عتاداً، أو مجالاً في تنفيذ اعتداء أو هجوم على الغير قد يتناول موارده السيبرانية أو أدواته التي يوظفها للحضور في الفضاء الافتراضي، أو قد تتجاوز بتأثيرها لتشمل أي أداة تتواصل مع مختلف أشكال عقد الفضاء السيبراني.

وكما أن الحروب والتعرضات التقليدية قد تحفل بهجمات برية، أو بحرية، أو جوية، كذلك أضحت الهجمات السيبرانية جزءاً لا يتجزأ من استراتيجية المواجهة بين المتخاصمين في مجال الفضاء السيبراني الافتراضي، والذي فرض حضوره قبالة مجالات المواجهة البرية والبحرية والجوية، على حد سواء (*Nguyen,2013*).

فالهجمة تبقى لصيقة بهوية، وتوجهات، وغايات الجهة التي تمارسها (سواء كان شخص، أو مجموعة، أو مؤسسة). كما أن هوية المورد السيبراني الذي تستهدفه تؤثر الى حد كبير في تمييز مختلف أشكال الهجمات السيبرانية، يضاف الى ذلك طبيعة الحافز الذي دفع بالمهاجم الى مباشرة عملية التعرض أو الهجمة على الكائن السيبراني المستهدف، ثم يأتي دور حجم الخلل الذي أحدثته الهجمة على موارد الخصم في تحديد هويتها وانتمائها، اما الفسحة الزمنية التي تمتد عليها الهجمة فلها دور كبير في ترسيخ وجود هجمة معلوماتية، متى كان الزمن المستغرق لتنفيذها وديمومة تأثيرها، كافياً لإحداث تأثيرات ملموسة على الكيانات والعقد السيبرانية التي تستوطن في فضاء الخصم (*Kadivar,2014*).

ويشترك المجال الافتراضي الجديد مع بقية مجالات المدافعة والمنازعة التقليدية بوجود تخوم مشتركة، قد تجمعه معها بحيث يمتد تأثير الهجمات التي تسري في فضائه المتخيل ليطال تأثيرها أدوات ومعدات تقيم في المجال البري، أو البحري، أو الجوي، نتيجة لوجود عقد رقمية تصل مجال فضائه المتخيل بمجالاتها الفيزيائية.

وتستخدم الحواسب وأدوات الاتصالات بوصفها أدوات تستبطن قدرات لممارسة فعاليات تلصصية توطئ لهجمات يستهدف بها الخصم من خلال إحداث خلل، أو تشويش، أو تدمير (جزئي أو كلي) في النظام الذي يدير مجاله الافتراضي، أو نسيجه الشبكاتي، او الموارد والمستودعات السيبرانية المرتبطة به، أو عقد معلوماتية محددة تمتلك خاصية ذات بعد استراتيجي، عسكري أو سياسي، أو خدمي مؤثر(*Reyes,2007*).

وتتألف الهجمة السيبرانية من مركبتين أساسيتين، عملية الكشف عن الثغرات الأمنية[119] المقيمة في الهدف، وانتخاب مستوى الزخم[120] *Payload* الذي يمكن اعتماده لاستثمار الثغرة والولج الى ساحة النظام لتحقيق إصابة أكيدة للعقد والكيانات السيبرانية المستهدفة. وقد تتضمن الهجمة إجراءً أو مجموعة إجراءات تشمل: زج شيفرات برمجية، أو إلغاء مقطع محدد من البيانات، أو إحداث تغييرات في مسارات تنفيذ العمليات البرمجية لإحداث التأثير المشوّش وتناسل تأثيراته في نسيج النظام لتحقيق المستوى التخريبي الذي يروم المتسلل إحداثه في الهدف. ومن الممكن طمر هذه التغييرات وربطها بمحددات زمنية، أو أخرى ترتبط بتسلسل منطقي يضمن إحداث ضرر أكبر خلال بعد زمني محدد، أو عند إجراء عمليات محددة ترتبط بخوارزمية حاكمة لأداء النظام (*Nguyen,2013*).

وتتنوع أشكال الهجمات السيبرانية، وتتباين نزعاتها نتيجة للتباين الكبير في معمارية النظم البرمجية، ومكونات النسيج الشبكاتي، واتنوع العقد السيبرانية، ومستويات تحصين الجدران النارية، مع تنوّع نهج قراصنة المعلومات في تجاوز العقبات المتكاثرة أمام حركتهم في المجال السيبراني المستهدف. من أجل هذا سنسعى الى تقسيمها وتبوبيها الى مجاميع يلتحق بكل منها طيف واسع من الهجمات التي تنصبغ كل منها بصبغتها الفريدة التي تفرضه خصائص البيئة والنظام البرمجي، من جهة، والعمق المعرفي لقرصان المعلومات ونهج تعامله مع الثغرة السيبرانية لكل حالة من الحالات التي تتضمنها الهجمة السيبرانية.

قسم الباحث (*Nguyen,2013*) الهجمات السيبرانية الى صنفين أساسيين:

الصنف الأول: هجمات اختراق *Penetration Attacks* تتضمن سلسلة من أنشطة التسلل والولوج الى حمى النظام السيبراني ونسيجه الشبكاتي عبر ثغرة مقيمة في نسيج النظام أو إحدى صفحات تطبيقاته البرمجية.

الصنف الثاني: هجمات رفض الخدمة (*DoS*) *Denial of Service Attacks* التي تهدف الى خلخلة وتشويش سريان الخدمة لزوار الموقع ومستثمري المحتوى السيبراني المطروح على صفحاته من خلال إغراق الموقع بسيل من طلبات الخدمة التي تؤدي الى حصول اكتظاظ كثيف في مضيفات الموقع يحول دون قدرتها على تلبية طلبات الزوار والمستخدمين نتيجة للشلل الذي ينشب عن سيل الطلبات التي يلفقها المهاجمون.

وتنتظم تحت مظلة هذين الأسلوبين من الهجمات السيبرانية، مجموعة متنوعة من الممارسات السيبرانية التي يحاول أصحابها إحداث تأثيرات مزعجة، أو ضارة، أو تدميرية في الكيانات السيبرانية (سواء كانت حواسب، أو مضيفات خدمة، أو إحدى و/أو جميع مكونات النسيج الشبكاتي لنظام من النظم) (*Colarik,2006*).

ويعمد المهاجمين (ممن يخترقون نظم المعلومات) الى طمر برمجيات خبيثة *Malware*، تحتوي على شيفرات برمجية ينشب عن تنشيطها حصول خلل في الأداء، أو تشويش في سريان الأنشطة ضمن بيئة النظام، أو استلاب ملفات وبيانات مهمة. وتتميز بعض البرمجيات الخبيثة بقدرتها على التناسل وتوسيع نطاق وجودها في نسيج النظام الشبكاتي، والكشف عن ثغرات جديدة لإدامة زخم الهجمات، وتوسيع دائرة تأثيراتها (*Janczewski&Colarik,2008*).

[119] . الثغرة الأمنية عبارة عن موطن ضعف في بنية النظام، أو بيئته البرمجية، تتيح للقرصان السيبراني فرصة ثمينة للولوج الى النسيج الشبكاتي وممارسة الهجمة على إحدى كياناته السيبرانية، وتحقيق غاياتها. وقد تنشأ الثغرة السيبرانية عن وجود خلل في تصميم عتاد الحاسب، أو وجود فراغ في البيئة البرمجية، أو غياب بعض معايير السلامة عن الشبكة بحيث يمكن أن تستثمر إحداهما أو جميعاً للدخول الى حمى النظام والتمتع بصلاحيات وتخويل يرقى الى مستوى التأثير على جزء أو جميع مكونات النظام.

[120] . مستوى الزخم يصف حجم الممارسات السيبرانية المطلوب تنفيذها لضمان استثمار الثغرة السيبرانية المتاحة لبلوغ إصابة أكيدة وإحداث تأثير معنوي على الهدف.

وتنتمي الى قائمة البرمجيات الخبيثة التي يزرعها المهاجمون في تربة البيئة السيبرانية لفضاء الفيض السيبراني كل من: الديدان السيبرانية[121] *Worms*، وبرمجيات حصان طروادة[122] *Trojan Horse*، وفايروسات الحاسب[123] *Computer Viruses*، والنغفة السيبرانية[124] *Bot* (*Nguyen,2013*).

ويلتحق بالصنف الأول مجموعة الأنشطة التي يحاول المهاجمون من خلالها اختراق صفحات الويب *Web Defacement*، لإطلاق خطاباتهم السياسية أو شعارات مجاميعهم التخريبية ضمن صفحات الويب الحكومية، أو تلك التي تعود الى شركات تجارية، أو شخصيات مرموقة، بقصد نشر دعاية لحركتهم أو إحداث خلل في مظهر ومحتويات صفحة الويب المخترقة، أو تراجع أداء مكوناتها (*Janczewski&Colarik,2005*).

5. 3. حروب فضاء الفيض السيبراني:

شاع استخدام اصطلاح حرب الفضاء السيبرانيي *Cyber Warfare* لوصف نمط من الممارسات العدوانية ـ السيبرانية التي تتجاوز في تأثيراتها الضارة عتبة التأثير الذي ينشأ التهديدات والهجمات التي يلاحظ حضورها بشكل لافت في فضاء الانترنيت، وتمتد تأثيراتها في النسيج السيبراني للشبكات المحلية والعولمية (*Green,2015*).

بصورة عامة لا يمكن تشكيل تعريف دقيق لهذا النمط من النزاعات المستحدثة ما لم نشرع في تحليل مادة المجال المتخيل والذي يتميز بسمات فريدة، مع وصف وبيان هوية الكيانات التي تفرض حضورها في هذا الفضاء، وتمارس طيفاً متنوعاً من أنشطة المنازعة، والمجالدة، والمنافحة، والمقارعة ضمن مواقع التخاصم السيبراني التي تحتضنها وتؤجج تأثيراتها الضارة و/أو التدميرية.

وتسهم سمة الانفتاح، وتنوّع الموارد السيبرانية، وتباين هوية الكيانات السيبرانية والمتخيلة لقطان الفضاء السيبراني، مع تكاثر وتنوّع آليات ممارسة التهديدات والهجمات في كل نزاع من هذه النزاعات.

من أجل هذا تكاثرت التعريفات نتيجة اختلاف مضامين معالجة ميدان المخاصمة، والأدوات المستخدمة في المنازعة السيبرانية، وتباين هوية جحافل القوات السيبرانية، وطبيعة العقد السيبرانية التي تنالها آثار النزاعات بصور مباشرة، أو غير مباشرة (*DoD,2002*).

لا زالت أدبيات وزارة الدفاع الأمريكية تفتقر الى تعريف دقيق وشامل لوصف حروب فضاء الفيض السيبراني، رغم إقرار نائب وزير الدفاع الأمريكي بأن الفضاء السيبراني بات يشكّل مجالاً مضافاً لمجالات المواجهة العسكرية في الألفية الجديدة (*Andress, et.,al.,2014*).

---

[121] . الدودة السيبرانية برنامج خبيث يتميز بحضوره المتفرد، وقدرته الفريدة على التناسل وتوليد المزيد من أفراد أسرته الخبيثة. ويؤدي التكاثر المستمر في إحداث خلخلة بأداء النظام بالإضافة الى المهام الأخرى التي قد أودعت في نسقه البرمجي.

[122] . حصان طروادة تطبيق برمجي خبيث، لا يوحي تشغيله بوجود سلوك أو تنفيذ مسار برمجي غير مشروع، ولا يقوم بعملية تكاثر داخل حدود النظام، بينما يحرص على التخفي في النظام البرمجي لضمان تنفيذ المهام المدرجة في معماريته البرمجية وتعميق التأثيرات الضارة في الحواسب والنظم المستهدفة دون لفت نظر المستخدم الى حضوره.

[123] . فايروس الحاسب برنامج خبيث يلجأ الى إصابة الحاسب أو النظام السيبراني عند تشغيله ليباشر بالالتصاق بتطبيقات برمجية، أو الحضور المستديم في ذاكرة الحاسب مما يؤدي الى تباطؤ الأداء، أو ممارسة سلسلة من الأنشطة التخريبية التي قد تؤدي الى إتلاف بيانات، أو التأثير على التطبيقات البرمجية أو إتلاف بعض الأجزاء من عتاد الحاسب ومستودعاته السيبرانية.

[124] . النغفة السيبرانية برنامج خبيث يعد من أكثر البرمجيات التي تهدد استقرار شبكة الانترنيت، وتسهم في زلزلة أركان أمنها. وتمنح هذه البرمجيات، قائد الهجمة *Bot Master* فرصة بسط نفوذ أعضاء فصيله السيبراني، وإحداث التأثيرات الضارة من خلال إقحام الفايروسات أو الديدان أو خيول طروادة داخل نسيج النظام المستهدف. ويستطيع المهاجم إدارة عمل النغفة عن بعد فيمارس ما يشاء من تأثيرات ضارة عبر العقد السيبرانية لنسيج شبكة الانترنيت.

من أجل هذا نلحظ أن التعريف الشائع لهذا النمط من الحروب لا زال مقارباً للتعريف الذي أطلقه *Clausewitz* على الحرب التقليدية[125] مع إحداث تغيير طفيف على بعض المفردات ذات الصلة بالفضاء السيبراني المتخيّل، عندما نراجع أكثر التعريفات شيوعاً والذي اقترحه أحد خبراء مكافحة الإرهاب في البنتاغون، عندما عدّها مجموعة من الأنشطة التي تمارسها الدول للتوغّل في فضاء حواسب أو شبكات المعلومات التي يمتلكها الخصم بقصد إحداث خلل في أدائها أو تخريب في نسيجها ومكوناتها (*Knopova&Knopova,2013*). وقد تبنت، أخيراً، وزارة الدفاع الأمريكية (البنتاغون) تعريفاً جديداً لحرب المعلومات *Cyber Warfare* فأطلقت الاصطلاح على مجموعة الأنشطة التي توظف فيها السطوة السيبرانية *Cyber Capability* (المتمثلة بالحواسب وعتاد شبكات المعلومات، والنظم البرمجية) لتحقيق أهداف عسكرية وإحداث تأثيرات مؤثرة على الخصم ضمن مجال فضاء الفيض السيبراني (*Chopitea,2012*).

أما البيئة الصينية فقد ترعرع في تربتها تعريف آخر لهذا المصطلح، حيث ذهب رئيس وزارة الاتصالات *Xu Xiaoyan* الذي حصر حروب فضاء الفيض السيبراني بالنزاعات التي توظف التقنيات الشبكاتية في ممارسة عمليات مقاطعة فيض البيانات السيبرانية، وإحداث تشويش وخلل مؤثر في محتواها، وتدمير البنى التحتية للمعلومات والاتصالات للخصم من خلال زج بيانات مضللة، ونقل فايروسات الحواسب، والديدان السيبرانية، على التوازي مع توظيف القدرات التأثيرية لطيف واسع من الأدوات السيبرانية التي تستوطن النسيج الشبكاتي للخصم بحيث تورث نظامه السيبراني المزيد من الآثار المدمرة بصورة جزئية أو كلية (*Hwang,2012*).

من جهة أخرى كان لحلف الناتو[126] موقفاً في تحديد دلالة اصطلاح حروب فضاء الفيض السيبراني أنها نمط من أنماط النزاعات التي تستعر في الفضاء الافتراضي وبتوظيف آلات وأدوات تقنية المعلومات والاتصالات السيبرانية. وذهبت الى أن هذا النمط من الحروب يمكن أن يعد جزءاً ملحقاً بالعمليات العسكرية التي تسود في المجالات البرية، والبحرية، والجوية. وتتميز هذه الحروب بتوظيف تقنيات رقمية متقدمة، حيث العمليات المحوسبة التي تسري سطوتها في النسيج الشبكاتي للشبكات المحلية وشبكة الانترنيت.

أما روسيا الاتحادية فترى أن هذا النمط من الحروب عبارة عن نزاعات رقمية بين الدول تستهدف نسيج البنية التحتية للمعلومات والاتصالات للعدو كجزء من الحملة العسكرية الواسعة التي يتضمنها النزاع العسكري بين الدول المتحاربة (*Godwin,2014*).

وإذا أردنا أن نخلص الى تعريف جامع لحروب فضاء الفيض السيبراني فليس أمامنا سوى الاعتراف بأن هذا النمط من الحروب لا يستأثر بمفرده بساحة المنازعة بين الأطراف المتناحرة، وإنما يغطي جزءاً محدوداً منها، ويشكّل عنصراً مضافاً الى بقية صنوف المواجهة التي تتخذ من البر، أو البحر، أو الجو، أو الفضاء مجالاً لامتداد تأثيرها على ساحة المنازعة. وأن جوهر اختلافه عن بقية أصناف المواجهات التي تسري في ساحة الحروب أنه يستخدم فضاء الفيض السيبراني مجالاً لممارسة التهديدات والهجمات على العدو، ويستهدف النسيج الشبكاتي للعدو والكيانات السيبرانية، الفيزيائية منها والمتخيلة التي تستوطن هذا الفضاء، والذي يعد مظهراً مستحدثاً لمجال المنازعة.

إذن لا يمكن القطع بحدوث حرب معلوماتية شاملة لغاية هذا التاريخ رغم ازدحام سجلات الفضاء السيبراني بإعداد متنامية من التهديدات والهجمات السيبرانية التي تحفل بها وقائع عصرنا الراهن، وتقتصر الوقائع على أنماط متباينة

---

[125] . الحرب بحسب تعريفه التقليدي هي مبدأ ممارسة القوة لإجبار عدونا على الانصياع لإرادتنا.

[126] . تبنى مركز دفاع فضاء الفيض السيبراني لحلف الناتو هذا التعريف *NATO Cooperative Cyber Defense Centre of Excellence*، راجع الموقع: *https://ccdcoe.org/cyber-definitions.html* .

من التهديدات والهجمات المنفردة أو المجتمعة، والتي لم يرقى أي منها الى مستوى يمكن أن نطلق عليه اصطلاح حرب رقمية.

بيد أن تزايد حضور تقنيات المعلومات والاتصالات وأدواتها في مجتمع المعلومات والمعرفة المعاصر، وتداخل عمليات إدارة أنشطة قطاعات المجتمع المختلفة، وتغلغل البنية التحتية للمعلومات والاتصالات على عموم الرقعة الجغرافية العولمية سيعمّق من الدور الذي يمكن أن تمارسه أنشطة المنافحة والمدافعة السيبرانية في إدارة ملفات النزاعات الإقليمية، والدولية المحتدمة بين الكيانات السياسية المتصارعة (*Erbschloe,2001*).

أما على صعيد حصول حرب معلوماتية وفق المفاهيم والسياقات العسكرية والتعبوية، فإن هناك ثمة اتفاق بين المتخصصين في مجال التهديدات والهجمات السيبرانية على أن بداية عصر نزاعات فضاء الفيض السيبراني قد بزغت بشكل ملحوظ خلال النزاع المحتدم في استونيا عام 2007[127]، ثم النزاع الذي نشب عام 2008 في جورجيا. بينما عدّت ولادة هجمة الدودة السيبرانية[128] *Stuxnet* بداية لعهد جديد من هجمات الذكاء المحوسب، والذي اتسمت معماريته البرمجية والمنطقية بتعقيد من نمط مستحدث بات ينذر بولادة نمط غير مسبوق من التهديدات والهجمات السيبرانية في دائرة البرزخ الذي يصل الفضاء المتخيّل بالفضاء الفيزيائي لحياتنا اليومية (*Green,2015*).

نشبت الأزمة الاستونية عام 2007 نتيجة للخلافات المستفحلة مع روسيا الاتحادية، والتي اتخذت طابعاً إثنياً في ظل سلسلة من الاعتصامات والاضرابات. بيد أن تحولاً هاماً قد حصل في مجريات هذه الأزمة عندما تعرّضت البينة التحتية للاتصالات والمعلومات، والمواقع الحكومية، وماقع المصارف والمؤسسات المالية والاقتصادية الى سيل هادر من هجمات رفض الخدمة *DDoS* التي أغرقت هذه المواقع بواسطة هجمات قد نشأت عن أكثر من 80,000 عنوان (*IP Address*) لعقد رقمية مارست هذه الهجمات على المواقع الحيوية في إستونيا (*Green,2015*).

ابتدأت هذه الهجمات في 27 من شهر أبريل من عام 2007، وقد امتدت هذه الهجمات فنالت شبكات هواتف المحمولة لأعضاء البرلمان الاستوني، والمضيفات الأساسية للمؤسسات الحكومية، ومكتب الرئيس. واستمرت هذه الهجمة في إحكام قبضتها على نظم المعلومات والاتصالات الاستونية لبضعة أسابيع.

وقد حفلت المنتديات السيبرانية لقراصنة المعلومات في روسيا بأدوات وتطبيقات تدعم المستخدمين الداعمين لنهج روسيا الاتحادية مع إرشادهم الى الأهداف المهمة التي يمكن أن تستهدف عند إنشاء المزيد من هجمات رفض الخدمة لضمان استمرار حالة الحصار السيبراني، وترسيخ الشلل شبه التام في منظومة المعلومات والاتصالات الاستونية.

وجّه الرئيس الاستوني أصبع الاتهام نحو الإدارة الحكومية في روسيا الاتحادية، وذكر أن الكرملين قد أجج النزاع من خلال تجنيد عدد كبير من المواطنين الروس والمناوئين للمشاركة في حملة مشتركة لتأجيج عدد كبير جداً من الهجمات السيبرانية على إستونيا، والتي عدّت حرباً معلوماتية مصغرة استهدفت إستونيا (*Allison,2008*).

وقد اضطرت السلطات الاستونية الى الاستعانة بخبرات متخصصين في أمن المعلومات من إسرائيل ودول حلف الناتو لتجاوز التأثيرات الضارة لهذه الهجمات وعبر سلسلة من الإجراءات التي سعت الى الارتقاء بالكفاية الأمنية لشبكات المعلومات بالبلاد.

---

127 . أطلقت مجلة *Economist* (على الهجمات السيبرانية التي استهدفت استونيا) حرب الويب الأولى *Web War I* ، بينما أطلق عليها أخرون حرب فضاء معلومات استونيا (*Rowen,2015*).

128 . أرجأنا مناقشة دودة Stuxnet الى فصل لاحق كونها ولادتها قد حصلت في الفضاء السيبراني الإيراني واستهدفت المشروع النووي الإيراني دون غيره.

وقد تكرر المشهد ثانية أثناء السجال السياسي والعسكري بين جورجيا وروسيا الاتحادية عام 2008 حيث تكاثرت الهجمات السيبرانية قبل شهر من نشب النزاع العسكري بين البلدين. وقد وصلت آثار هذه الهجمات الى موقع الرئيس الجورجي فأغرق بسيل من بحزم رقمية متنوعة سببت في توقف الموقع لأكثر من 24 ساعة قبل أن يستعيد عافيته ويعاود عمله ثانية (*Green,2015*).

كانت الهجمة الأولى في بدايات شهر يوليو، وقد تلتها هجمة أخرى، أكثر شراسة في الأسبوع الأول من شهر أغسطس من العام ذاته. وقد نشب عن سلسلة الهجمات الجديدة تعطيل عمل جميع مواقع الويب التي تستخدمها جورجيا في التواصل مع مواطنيها ودول العالم. ثم امتد تأثيرها الى المواقع الحكومية، ومواقع المؤسسات المالية والاقتصادية في عموم البلاد، في خطوة للضغط على الحكومة الجورجية مع استمرار النزاع بينها وبين روسيا الاتحادية.

اضطرت السلطات الجورجية الى الاستعانة بخبراء من جارتها استونيا والتي تعرضت لهجمات مماثلة قبل عام، كما وفرت السلطات البولندية فضاء رقمياً لاستضافة موقع الرئيس الجورجي لحين تجاوز آثار الهجمات ضد بنيتها التحتية للمعلومات والاتصالات.

وتميزت هذه الهجمات بوقوعها على التوازي مع النزاع العسكري المحتدم بين البلدين، مع إحداث إعاقة وشلل في أداء الكثير من المؤسسات الحكومية والاقتصادية والخدمية في عموم جورجيا، الأمر الذي رسّخ فرص تكامل جبهات النزاعات العسكرية في المستقبل بعد انضمام جبه حروب المعلومات الى بقية جبهات المواجهة، ونجاحها في إحداث تأثيرات تشابه الى حد كبير تلك التي تنشأ عن الحروب التقليدية (*Green,2015*).

لا زال مفهوم حروب الفضاء السيبراني تلفّه سحابة من الغموض والابهام، وتتقاذف خطاطته الكثير من الإشكاليات المعرفية. ذلك لأن معظم الوقائع والشواهد التي تتوفر بين أيدينا تكاد تخلو من سيناريو متكامل لمعركة (بالمفهوم العسكري) قد نشبت على أرض فضاء الفيض السيبراني، وأن جل ما يتوفر لدينا عبارة عن ممارسة سيل من التهديدات والهجمات السيبرانية التي بدأت بالتطور خلال العقدين الأخيرين من هجمات منفردة وغير منسقة الى هجمات تتسم بتنسيق عال، وبمشاركة أكثر من جهة، ومن عقد معلوماتية تستوطن فضاءات متعددة. بيد أن هذه الإشكاليات، لا يمكن أن تنفي إمكانية حدوث حروب معلوماتية بين مراكز قوى، في المستقبل المنظور نتيجة لتعاظم الدور الذي بات يمارسه فضاء الفيض السيبراني في حياتنا المعاصرة، والدور الذي بات يمارسه على صعيد توازن القوى بعد أن أثبتت التقارير والدراسات وجود توجّه محموم نحو ممارسة عمليات التعرض والتهديد السيبراني على مستوى الدول المتنازعة، وبصورة معلنة، في بعض الأحيان، كما هو الحال في النزاع المستديم بين الولايات المتحدة وإسرائيل مع إيران.

وإذا حاولنا مراجعة مفهوم الحروب التقليدية في مصادر العلوم العسكرية، سنجد أن هذا المصطلح قد تكرر استخدامه لوصف صراع بين جهتين متناحرتين تستخدم فيه أدوات الحروب ، سواء كان الصراع على مستوى دول، أو مدن، أو قبائل، أو مجاميع متناحرة.

وإذا كانت الحروب التقليدية قد مرت بسلسلة من التحولات بحيث أضحت أنشطتها تمارس في الفضاء، بعد أن أحكمت قبضتها على اليابسة، والبحار، والسماء، فإن النزاعات في عصر المعلومات قد نقلت مجالها الى الفضاء الافتراضي ـ المتخيّل، وفتحت أكثر من جبهة للنزاع بعد أن شهدنا ولادة الحروب الالكترونية *Electronic Warfare*، وحروب قراصنة المعلومات *Hackerwar*، وحروب اقتصاد المعلومات *Information Economic Warfare*، وحروب فضاء الفيض السيبراني *Cyberwar*.

ورغم اختلاف مسميات هذه الأنماط الجديدة من الحروب فإنها تتفق في توظيف فضاء الفيض السيبراني بوصفه مجالاً لممارسة التهديدات ومباشرة الهجمات، كما أن أنشطتها تستهدف الكيانات السيبرانية ومواردها المقيمة في الفضاء السيبراني المتخيّل.

6 . الجماعات المتخيلة التي تنشط في فضاء المواجهة والمدافعة:

يحضر في المجال المتخيّل الذي تسوده النزاعات السيبرانية طيف واسع من المستخدمين (أفراداً ومجاميع، ومؤسسات) الذين يمارسون جزءَ محدوداً، أو جلّ النشاطات والممارسات التي تسوده للتعبير عن وجه من أوجه النزاع المحتدم بين الخصوم، أو المتنافسين على موازين القوى الناعمة التي تحكم سيطرتها على فضاء الفيض السيبراني، أو الفضاء التقليدي.

ولم تعد تقتصر وصلات المستخدم بالفضاء السيبراني على الحواسب المكتبية أو الحواسب المحمولة، بعد أن ارتبطت الحواسب اللوحية، والهواتف المحمولة بالفضاء ذاته، وعبر وصلات رقمية أكثر مرونة وانفتاح. لقد توسع المجال الاتصالي، وتكاثرت العقد والكيانات السيبرانية المرتبطة بفضاء الفيض السيبراني، وتشابكت خيوط نسيجه بحيث أصبحت المنافذ المتاحة للولوج الى هذا الفضاء المتخيّل، سواء كانت عملية الدخول مشروعة، أو غير مشروعة.

يضاف الى ذلك وجود تباين شديد بين غايات المستخدمين، وتنوّع مبررات حضورهم في الفضاء المتخيّل، الأمر الذي يزيد من تعقيد عملية تتبع بزوغ التهديد الأمني، ومسارات تطوره باتجاه هجمة حقيقية، أو ممارسة جريمة معلوماتية *Cybercrime*، أو كونه بداية لسلسلة من الهجمات المتلاحقة التي تورث الكيان السيبراني المستهدف المزيد من الآثار الضارة أو التدميرية.

وشأن الاتساع والانفتاح غير المسبوق الذي يتصف به فضاء الفيض السيبراني، فإن سمة المرونة غير التقليدية تكاد أن تسم تراتبية حضور المستخدم في هذا الفضاء، بعد أن وفرت له منصات التطبيقات فرصة تقمّص أكثر من هوية حضور بالوقت ذاته، ومنحته قناعاً رقمياً Avatar، يستطيع أن يغيّب وراءه هويته الحقيقية، والغاية من حضوره في طبقة من طبقات هذا الفضاء، مما يصيب من يحاولون تتبع الاستحالات التي تمر بها الهوية السيبرانية باليأس والقنوط من إمكانية الإمساك بتلابيب علامات حضوره السيبراني وتحديد بصماته الحقيقية.

ولن نحاول أن نكشف اللثام عن هوية جميع الكيانات التي تقطن في فضاء الفيض السيبراني، وسنحصر اهتمامنا فقط بالفئة الناشطة على صعيد ممارسة مختلفة أشكال التهديدات العسكرية أو الأمنية، أو ممارسة الجريمة المنظمة، لنلقي الضوء على الكيانات التي تقيم في الجزء المظلم من الفضاء المتخيّل، وتمارس نشاطاتها في دهاليزه السحيقة.

أحسن الباحثان *Aghili&Kahnegi* صنعاً في لململة هويات الكيانات التي تقيم في الجزء المظلم من فضاء الفيض السيبراني وتصنيفها في جدول جامع يحدد ملامح حضورها مع تبيان الحافز الذي دفعهم للحضور في هذا الجزء من الفضاء المتخيّل، مع تبيان طبيعة الأهداف التي تستأثر باهتماماتهم، والنهج الذي يوظفونه في ممارساتهم العدوانية تجاه الآخر (*Aghili &Kahnegi,2013*) ـ أنظر الجدول (4 - 12).

الجدول (4 - 12) ـ كشاف تفصيلي لهوية الكيانات المقيمة في الجزء المظلم من فضاء الفيض السيبراني.

هوية المقيم	الحافز أو الدافع	الهدف المنشود	النهج المستخدم
المستخدم العادي	دافع غير ناضج	هدف غير محدد	أسلوب غير مباشر
مستخدم يمتلك مهارات غير ناضجة.	حب الاستطلاع او للتشويق أو الاثارة والتظاهر بالمهارة والسطوة.	أفراد، شركات، أو مواقع حكومية متفرقة	استخدام شيفرات برمجية جاهزة أو تطبيقات بدائية مطروحة على مواقع الانترنيت
ناشط رقمي	السعي الى إحداث تغيير اجتماعي أو سياسي	صنّاع القرار أو ضحايا بريئة	ممارسة اعتصام رقمي عبر مواقع الويب، أو شلل عمل صفحة ويب، أو ممارسة هجمات رفض الخدمة
قرصان معلومات (ذو القبعة السوداء)	فرض الذات، أو مكاسب مالية أو اجتماعية	أي هدف	برامج خبيثة، فايروسات الحاسب، استثمار ثغرة أمنية
قرصان معلومات (ذو القبعة البيضاء)	تبني مبادئ مثالية، والرغبة في بسط سلطة القانون	أي هدف	فحص سلامة النظام والكشف عن الثغرات الأمنية لأصحابه لتلافي الاختراقات المحتملة
قرصان المعلومات (ذو القبعة الرمادية)	أمور ملتبسة	أي هدف	أساليب متنوعة
قرصان معلومات (ذو نزعة وطنية)	النزعة الوطنية	أعداء الأمة والبلاد وخصومها	هجمات رفض الخدمة، وشلّ مواقع الخصوم
ذوي معرفة بفضاء الفيض السيبراني	مكاسب مادية، انتقام أو الإعلان عن مظالم	رب العمل	هندسة اجتماعية، أو البوابات الخلفية، أو معالجات بارعة
إرهابيو فضاء الفيض السيبراني	إحداث تغييرات سياسية أو اجتماعية	ضحايا أبرياء	موجة عنف أو ممارسات تدميرية توظف الحاسب وادواته
منتجو البرمجيات الخبيثة	مكاسب مادية	أفراد أو شركات صغيرة	استثمار الثغرات الأمنية
مخادع معلوماتي	مكاسب مادية	أفراد أو شركات	هندسة اجتماعية
عصابات جرائم معلوماتية منظمة	مكاسب مادية	أفراد وشركات	برمجيات خبيثة للتهديد، أو سرقة الهوية السيبرانية، أو هجمات رفض الخدمة
مؤسسات	مكاسب مادية	نظم وشبكات معلومات وبنيتها	مدى واسع من أنماط الهجمات والتعرضات السيبرانية

هوية المقيم	الحافز أو الدافع	الهدف المنشود	النهج المستخدم
		التحتية الخاصة أو العامة	
عملاء تجسس معلوماتي	مكاسب مادية وسياسية	أفراد، شركات أو مؤسسات حكومية	مدى واسع من الهجمات السيبرانية
ميليشيات فضاء الفيض السيبراني	ذوي نزعات وطنية أو تنمية قدرات	أعداء الأمة والبلاد	تعتمد على القدرات والمهارات التي يمتلكها أعضاء الميليشيا.

المصدر: *Aghili &Kahnegi,2013*.

يوفر لنا الجدول مشهداً جلياً يصف بعناية تفاصيل ديموغرافية سكان هذا الجزء من فضاء الفيض السيبراني، والتي تتميز بتنوع وثراء يتناسب مع ثراء محتوى الفضاء السيبراني. وتكاد تتفق جميع الفئات المقيمة في هذا الفضاء بقدرتها على استغلال الثغرات الأمنية الملتصقة بمعماريته السيبرانية لممارسة أنشطتهم بمختلف الدوافع التي تتخفى وراء كل منها.

تكاد صبغة التكسب المادي وفرض السطوة أن تتفوق على بقية الدوافع التي تدفع هذه الكيانات بممارسة أنشطتها، والتي تدفعنا الى تقسيمهم الى مجاميع جديدة:

- ✓ مجاميع الجرائم السيبرانية الفردية والمنظمة، والتي ينتمي اليها كل من: مستخدمون يتمتعون بمهارات معلوماتية غير ناضجة، وقراصنة معلومات بالقبعات السوداء، والرمادية، وذوي المعرفة العميقة بفضاء الفيض السيبراني، ومنتجو البرمجيات الخبيثة، والمخادعون السيبرانيون، وعصابات المعلومات المنظمة، والمؤسسات المتنافسة، وعملاء التجسس السيبراني.
- ✓ مجاميع الناشطين السيبرانيين الذين يريدون الصدع بمبادئهم لإحداث تغييرات في مجتمعاتهم، أو نشر خطابهم الإصلاحي.
- ✓ مجاميع تندفع بدفعات الحس الوطني لمقاومة أعداء الأمة والبلاد بدءاً بمحاولات فردية، وانتهاء بتشكيل ميليشيات بعيدة عن نظام الحكم أو ملتصقة بمنظومته السياسية تندفع بحرارة الحس الوطني لمباشرة هجمات قد تلجأ الى خطاب العنف أو الإرهاب في بعض الأحيان.
- ✓ أفراد يستغلون وجود الثغرات السيبرانية لإرضاء غريزة الفضول، أو آخرين يرومون إسداء النصح للغير لدرء الأخطار عنهم مثل قراصنة المعلومات بقبعاتهم البيضاء.

وفي الوقت ذاته يكاد يفصح الجدول (4 - 13) عما ذكرناه، حيث تبوأت جرائم المعلومات المرتبة الأولى بين بقية التهديدات خلال السنوات 2011-2016 حيث تراوحت نسبها بين 36 % وتزايدت أعدادها لتبلغ 68 %. وجاءت بعدها بالمرتبة الثانية تهديدات القرصنة السيبرانية والتي (في المدة ذاتها) بين 14 % و39 %. بينما جاء التجسس السيبراني بالمرتبة الثالثة وبنسب تراوحت بين 2 % الى 12 %. وجاءت التهديدات والحروب السيبرانية ذات الصبغة السياسية بالمرتبة الرابعة وبنسب تراوحت بين 2 % و5 %.

الجدول (4 - 13) ـ أنماط التهديدات والهجمات السيبرانية في فضاء الفيض السيبراني خلال السنوات 2011-2016.

الفئة	نسب حصول التهديدات والهجمات السيبرانية المختلفة					
	2011	2012	2013	2014	2015	2016
جريمة معلوماتية.	36 %	54 %	53 %	60 %	68 %	62.7 %
قرصنة معلوماتية.	24 %	31 %	39 %	27 %	14.7 %	28 %
تجسس معلوماتي.	5 %	2 %	6 %	8 %	12 %	5.3 %
هجمات وتهديدات.	3 %	4 %	2 %	5 %	5.3 %	4 %
متفرقة.	32 %	9 %	…	…	…	…

المصدر: *Hackmageddon,2016*.

الفصل الخامس:

الكيانات السيبرانية الإيرانية المقيمة في فضاء النزاع السيبراني

الفصل الخامس: الكيانات السيبرانية الإيرانية المقيمة في فضاء النزاع السيبراني

1. الكيانات الإيرانية[129] في فضاء النزاع السيبراني:

يتميز فضاء النزاع السيبراني في إيران بفسيفساء تضم كيانات وعناصر متنوعة فرضتها مستويات حضورها المختلفة، والتي تتسم كل منها ببصمة فريدة شأن البلاد التي تسودها تيارات عاصفة تتأرجح بين قطبين أساسيين، يتبنى الأول غلواً بيّناً ويشدد في التعامل مع الآخر ويضع للهوية القومية والصبغة العقدية حدوداً لا يسمح بتجاوزها، ويحرص الثاني، ويفصح عن رغبة محمومة بالانفتاح على المجتمع العولمي دون قيد أو شرط، بينما يستقر بين القطبين شعب عريق يعتز بهويته، وتتعلق روحه بتراثه ويحرص على ممارساته العقدية، ويريد أن يجافي الغلو بطرفيه المتناقضين.

لذا أظهرت تحرياتنا في ديموغرافية قطّان فضاء النزاعات السيبرانية، بصمة لكل فئة من هذه الفئات، وبنسب حضور مختلفة، إلا أن الهيمنة على القطب الأول قد فرضتها الكيانات التي تدير المؤسسة العقدية والسياسية في البلاد، بينما تهيمن على القطب المناوئ أقليات قد تبنت مبادئ الحداثة الغربية، وحرصت على زجها في المجتمع الإيراني، بينما تمارس الأكثرية حضوراً متقطعاً، ينمو، أو يتراجع مع نمو، وتراجع الحس الشعبي قبالة ما يعصف بالبلاد بين الحين، والآخر، دون ان يكون له انتماء سوى الى تربة إيران، وأعماق الحضارة الفارسية التي قد توغلت جذورها الى أعماق سحيقة في تاريخ الإنسانية فنحتت عراقتها في الطبقات الجيولوجية لصخور أرضها وجبالها.

2. نزعة القرصنة السيبرانية في إيران:

إن حضور القرصنة السيبرانية في إيران لا تقتصر على كونها مزاولة فردية أو جماعية استنبتت في فضاء الفيض السيبراني تعبّر عن ممارسة اجتماعية، غير سوية، أو كونها ممارسة تعكس عوزاً مكثفاً الى إشباع حاجات في بيئة نفسية تفتقر الى عناصر التوازن في بعض جوانبها ولكنها أضحت سمة مميزة لنظام يولي اهتماماً بها، ويسعى الى رعايتها بقصد استثمار نتائجها لتحقيق غايات سياسية ونشر خطاطته العقدية.

يشترك قراصنة المعلومات الإيرانيين مع بقية القراصنة المقيمين في الجزء المظلم من فضاء الفيض السيبراني، بقواسم مشتركة، تدفع بهم باتجاه ممارسة أنشطة القرصنة السيبرانية. فمن الدوافع المشتركة: الرغبة المحمومة في إشباع الفضول، أو السعي الى الظهور والغلبة على الأقران، أو تعزيز الثقة بالنفس عند النجاح في اقتحام مواقع الغير، أو فك رموز الشيفرات البرمجية التي يستعصي على الكثير فك دلالاتها والافصاح عن هوية الرموز التي تتخفى وراء جدرانها النارية وبواباتها الأمنية، أو الرغبة بجمع الأموال عن طريق الممارسات غير المشروعة لصالحه أو صالح جهات أخرى تغدق عليه الأموال لتحقيق غايات محددة (*Patterson&Smith,2005*).

أما إذا حاولنا الحديث خارج حدود القواسم المشتركة، سنجد أن مزاولة القرصنة السيبرانية لدى الإيرانيين تعد ممارسة قدرية توغلت في طبقات بشرتهم فبلغت شغاف أرواحهم بعد أن أوصدت عليهم الكثير من الأبواب، وضيّق عليهم المجال المفتوح لفضاء الفيض السيبراني بحيث لا تتوفر أمامهم سوى مواقع محدودة، ومحتوى رقمي مشوّش نتيجة لعمليات التقطير السيبراني التي تزاولها أجهزة المراقبة والحظر.

ولقد فرضت ممارسة أنشطة القرصنة السيبرانية على مساحة واسعة من أفراد المجتمع الإيراني نتيجة لآليات المراقبة والحظر التي مارستها الإدارة الحكومية في إيران، منذ بدايات الألفية الجديدة على مستخدمي الانترنيت بالبلاد، بعد

[129] . آثرنا استخدام اصطلاح مصطلح الكيان دون غيره، كونه مصطلح يكثر استخدامه في بيئة المعلومات والاتصالات للإشارة الى أي مستوى من الحضور السيبراني في الفضاء السيبراني سواء كان الحضور عتاداً أو مجموعة مستخدمين يقيمون في عقد رقمية تنتشر على النسيج الشبكاتي لفضاء الفيض السيبراني.

أن استشعرت بوجود مخاطر قد تؤدي الى حدوث خلخلة في منظومة ثقافة الثورة الإسلامية، ونشر ممارسات تتعارض مع المنظومة الأخلاقية للدين الإسلامي الحنيف.

وتسهم النزعة القومية لدى المواطن الإيراني، وانتمائه العميق الى الحضارة الفارسية وثقافتها العريقة التي امتدت جذورها الى عمق بلغ بضعة آلاف من السنين، الى ممارسة القرصنة السيبرانية لدرء ما قد يهدد كينونته القومية بواسطة أعداء الأمة الإيرانية، أو محاولة ليثبت جدارة قراصنتها أسوة ببقية الأمم، دون أن يكون لديه انتماء الى طائفة او حزب من الأحزاب أو التيارات المعارضة في إيران[130]. كذلك وتغذي نزعة الانتماء الى المذهب الشيعي، والحرص على الانتساب والاصطفاف مع آل البيت، والانتماء عقدياً الى المؤسسة الحوزوية في إذكاء نزعة وصبغة ذات نكهة خاصة في ممارسات القرصنة التي تحرص على ممارستها شريحة واسعة من المستخدمين الإيرانيين للذبّ عن منظومتهم العقدية تجاه مواقع ويب ومادة محتوى مناهض تتكاثر بصماته داخل حدود فضاء الفيض السيبراني لمجموعة من الدول الإسلامية. ولا يغيب دور المشهد السياسي عن تأجيج نزعة القرصنة داخل حدود إيران بين أنصار النظام وثقافة الثورة الإسلامية، والمعارضة بشقيها المعتدل والعلماني، فيحتشد قراصنة الأطراف المتنازعة سياسياً في الفضاء السيبراني، من داخل حدود إيران وخارجها، ليمارسوا أنماطاً متنوعة من عمليات القرصنة، وتشويش مادة الخطاب السياسي المطروح على مواقع الانترنيت للتعبير عن موقفهم السياسي أو العقدي.

من جهة أخرى ، تعزّزت الحاجة الى ممارسة القرصنة السيبرانية، لدى المواطن الإيراني، عاماً بعد عام، نتيجة لانفتاح محتوى فضاء الفيض السيبراني على المزيد من المفردات المعرفية التي تداخل نسيجها مع المزيد من مفردات باتت تستوطن في مساحات ذات صلة بالتهديدات الناعمة لخطاطة الثورة، وأمن الثورة الإسلامية، ثم أمن عموم البلاد، قبل أن تتحول ممارسات الفضاء السيبراني الى تهديدات وهجمات رقمية قد تقوّض أمن وسلامة البلاد برمتها، والتي انعكست بصورة مباشرة على ممارسات الحظر والكف السيبراني فأضحت أشدّ تعقيداً، واكثر شمولاً، الأمر الذي أجبر المستخدم الإيراني على الولوج الى طبقات عميقة في مجال المعارف التي تفتقر اليها القرصنة السيبرانية لكي يلبي حاجاته المتزايدة من هذا الفضاء الفريد.

وقد تطور مشهد ممارسات القرصنة السيبرانية وازداد تعقيداً (على الساحة السيبرانية الإيرانية) بعد أن وجد النظام الإيراني نفسه مضطراً، الى ممارسة القرصنة السيبرانية، بعد أن تزايدت التهديدات والهجمات السيبرانية المتلاحقة، على البنية التحتية للمعلومات والاتصالات، التي تستوطن لدى إداراته الحكومية، ومؤسساته الأمنية، ومنشآته النووية والصناعية (*Walls,2015*).

لقد مرّت دلالات ممارسات القرصنة السيبرانية بسلسلة من التحوّلات المفاهيمية، وقفزت من ساحة الممارسات الاجتماعية غير المتزنة، والجرمية، الى ممارسة تعبّر عن حاجات حقيقية ترتبط بحق الانسان في نوال المعرفة واشباع حاجاته الطبيعية، ثم الى ممارسة ذات بعد وطني نتيجة لمساهمتها في درء المخاطر عن حمى البلاد، وحماية العقيدة من التشويه، وابعاد عدم الاستقرار عن البلاد عند درء مخاطر التهديدات التي تمارس بواسطة الهجمات الناعمة على فضاء البلاد المعرفي (*Williams,2014*).

---

[130] . اعترف أحد القراصنة الهواة الإيرانيين والذي يطلق على نفسه اسم *"Spiderhacker."* بأنه قد قام باختراق عدد لا بأس من مواقع الويب، لا لشيء إلا لأنه قد وجد في نجاحه بعملية الاختراق تأكيداً على قدرة قراصنة المعلومات الإيرانيين على إحداث تأثيرات موجعة بمواقع الغير، شأن بقية قراصنة المعلومات الذين ينتمون الى بلدان وقوميات أخرى (*Patterson&Smith,2005*).

3. مجتمع قراصنة المعلومات الإيرانيين وكياناته:

يتألف مجتمع قراصنة المعلومات في إيران من خليط متعدد الهويات، متباين الانتماءات، متكثّر الغايات والأهداف، ويتسم بثراء محتواه الى الحد الذي يتطلب إفراده بدراسة شاملة للكشف بدقّة عن محتواه الفريد الذي لا نكاد نجد له شبيهاً في بقية قطاعات الفضاء السيبراني العولمي.

ويمكن أن يعزى هذا الأمر الى الحضور الفاعل للحكومة الإيرانية، ومؤسسة الحرس الثوري الإيراني، والباسيج في بيئة هذا المجتمع وتبنيها لمبدأ الاحتضان، والدعم، ومحاولة استنبات عدد كبير من قراصنة المعلومات في فضائها المحلي لتقوية شوكة الحصانة السيبرانية تجاه التهديدات المستمرة، وإطلاق العنان أمام القراصنة لشنّ الهجمات على خصومها.

وقد منحت الحكومة الإيرانية ومؤسساتها الأمنية للقراصنة المحليين أكثر من فرصة لإنشاء منتدياتهم السيبرانية، والتواصل فيما بينهم، بقصد استنبات القدرات الإبداعية، وتعجيل ولادة جيل من القراصنة الإيرانيين ذوي المواهب الفريدة، كما تستمر بحملات تجنيد القراصنة ودعوتهم للالتحاق بكتائب القراصنة في جيش إيران السيبراني، أو الفصائل السيبرانية التي تعمل تحت مظلة الحرس الثوري الإيراني. كما أنها قد غضّت الطرف عن نشوء ميليشيات من القراصنة السيبرانيين المحليين، الذين يدينون بالولاء لتيارات محافظة، أو متطرفة في سبيل ضمان حضور تنوّع فريد من الفصائل وكتائب القراصنة السيبرانيين المحليين، وبصرف الصرف عن طبيعة انتماءاتهم، وولاءاتهم، ما دامت تصبّ في صالح النظام، وتهتدي بهدي ثقافة الثورة الإسلامية، وتحرص على الطاعة والولاء المطلق لتوجيهات المرشد الأعلى للثورة الإسلامية.

إلا أن هذا الحشد الكبير من قراصنة المعلومات المحليين لم يخلو من زغل نتيجة لمغادرة بعضهم دائرة الولاء المطلق، أو تغيير مسارات الانتماء باتجاه التيارات العقدية أو السياسية المعارضة، أو نتيجة لتوجهات شخصية صرفة، مما جعل الفضاء السيبراني الإيراني يشهد ولادات قراصنة معلومات جدد يمارسون أكثر من نهج في عمليات القرصنة، فيتأرجحون بين مناصرة النظام عندما يتعلق الأمر بدرء مخاطر عن بيضة إيران وأمنها، بيد أنهم لا يتورعون عن مهاجمة مواقع حكومية لأنها تضيّق الخناق على حضورهم السيبراني، أو بسبب ممارساتها الغير المبررة في قطاعات محددة من قطاعات الواقع الإيراني الذي يعاني من هيمنة ترهق النفوس.

نشب عن هذا النمو المطرد في أعداد القراصنة، وتنوّع مشاربهم وتوجهاتهم، والحضور المباشر للإدارة الحكومية، في بعض القطاعات، وغيابها في الأجزاء المظلمة من الويب التي تتكاثر فيها أعداد القراصنة المعارضين، حصول تجاذبات وتدافع مستمر، بين مختلف الفئات، فحمل معه نمطين من التأثيرات، تأثيرات إيجابية أذكت روح التنافس والتدافع بين الأطراف المتعارضة، فأسهمت في تطوير بيئة القرصنة في الفضاء الإيراني، والثاني خروج بعض القطاعات من هيمنة النظام ومؤسساته الأمنية نتيجة لعمليات التداخل، وحضور القراصنة في فضاء مظلم قد لا تفلح متحسسات النظام بالوصول إليها، بعد أن صلب عودها وانتصبت نتيجة للدعم المسبق في استنباتها من قبل النظام ذاته.

يتميز مجتمع المعلومات الإيراني بتجمهر عدد كبير من قراصنة المعلومات، الهواة والمحترفين، على ساحته المتخيّلة، والذين توجهت أنظارهم نحو ممارسة القرصنة السيبرانية نتيجة للآثار المتراكمة عن الرقابة الصارمة وعمليات الحظر، متعددة الطبقات، التي تحرص المؤسسة الحكومية على ممارستها بكثافة على عموم مساحة فضاء الانترنيت ومجالات تطبيقاته السيبرانية.

لذا أصبحت القرصنة ممارسة يومية لكل من يروم الولوج الى فضاء الانترنيت، ووصول المواقع التي يريدها، بعيداً عن جدران الحظر، ومجسّات الرقابة التي قد طمرتها إدارة المعلومات والاتصالات في كل موطئ قدم من فضاء الفيض السيبراني بالبلاد.

وقد ازدهر مجتمع القراصنة مع تكاثر أدوات الاختراق التي تطرح على مواقع الانترنيت بالمجان، وازديدا أعداد خريجي الجامعات التقنية، وكثرة المواقع والمنتديات الإيرانية التي توجه اهتمامها نحو تطوير مهارات القرصنة، ودعم ممارساتها داخل حدود البلاد وخارجها، الأمر الذي أسهم في توسّع دائرته، وتعدد الفئات التي تنتمي اليه، وتحوّل تدريجياً من أداة بدائية يوظفها المستخدم للقفز فوق جدار حظر، وبلوغ موقع يثير اهتمامه، الى أداة أشد تعقيداً تستخدم في نشر خطابات المعارضة التي تناهض الحكم، أو تشويش خطابات النظام التي تطرح على مواقعه المختلفة، ثم تحوّل الى أداة تستخدمها جميع الأطراف المتصارعة (الحكومة، والمعارضة، والحكومات المناهضة للثورة الإسلامية) لدرء المخاطر، أو ممارسة سلسلة هجمات لخلخلة عمل المواقع، أو نشر بيانات سرية، أو إحداث خلل في أداء منظومات الاتصالات، والنقل، والصناعة، وغيرها من القطاعات الحيوية.

لقد توسع مفهوم القرصنة في إيران، وتحوّل من ممارسة غير مشروعة يعاقب عليها القانون، الى ممارسة تحتضنها الإدارة الحكومية وتطور مهارات أصحابها، وتوظف قدراتهم في الذب عن الحياض السيبرانية للبلاد، أو ممارسة هجمات شرسة ضد أعداء الأمة الإيرانية وخصومها.

من أجل هذا تكاثرت أعداد أفراد مجتمع القرصنة السيبرانية في إيران، وتنوعت هويتهم وانتماءاتهم، واختلطت أوراقهم بين مناصر للنظام وداعم لخطابه السياسي والعقدي، وبين معارض يلهج بخطاب معارض لثقافة الثورة الإسلامية، وفئة تمارس القرصنة بعيداً عن أنظار المعسكرين المتناحرين كي تمارس القرصنة في ممارسة سلسلة من جرائم الاحتيال والسرقة.

ورغم هذا الأمر، أو ذاك يستمر مجتمع قراصنة المعلومات في إيران بالنمو السريع، مع تكاثر سمة التنوّع لدى فئاته، مع تعمّق خبرات أفراده، وتزايد مستويات سلطانهم السيبراني، بحيث أصبح لهذا المجتمع شأناً كبيراً، وباتت الأنظار تتجه نحوه، من القاصي قبل الداني، وتتكاثر الأبحاث والدراسات التي تقوم بها مراكز الأبحاث والدراسات المتخصصة بمضمار أن المعلومات، والقرصنة السيبرانية بعد أن تزايد سلطانه، الى مرتبة، جعلت من هذا المجتمع مصدراً حقيقياً للتهديد السيبراني، على مستوى المنطقة، وعلى مستوى الفضاء السيبراني العولمي.

3. 1. مجاميع القرصنة السيبرانية في إيران:

تمتلك إيران مجتمعاً فريداً لقراصنة المعلومات، يتميز بتنوع هوية أفراده وتمتد على طيف واسع يلتحق بصفوفه ثلة من المستخدمين العاديين، أو أعضاء يعملون في شركات أمنية، أو مراكز بحوث، ثم ترتقي الى أفراد ينتمون الى مؤسسات حكومية ينصبغ نشاطها بصبغة عسكرية، أو امنية، أو أكاديمية صرفه. وتتباين مهاراتهم متدرجة من أضراب بدائية، لقراصنة مبتدئين، يوظفون أدوات بدائية تتسم بهيكلة مبسطة، وتطرح بالمجان على مواقع الانترنيت تدعم المستخدم العادي في ممارسة قفزات محدودة لتجاوز جدار أمني، أو عقبة أمنية ابتدائية، وتتطور هذه الخبرات لتبلغ لدى طبقة الصفوة، ممن اتقنوا مهارات القرصنة، ونجحوا بصناعة أدوات قرصنة احترافية، تسعفهم في العثور على ثغرات أمنية لم يسبقهم بقية القراصنة بالوصول اليها، فتشكل هجماتهم تهديداً وخرقاً خطيراً لنظم المعلومات التي تقع تحت طائلة نقراتهم الماهرة.

وسنحاول التعرّف على أكثر مجاميع القرصنة السيبرانية شهرة في إيران، ومجتمع القرصنة العولمي، في الفقرات القادمة للوقوف على توازن القوى داخل حدود مجتمع القرصنة في البلاد، وحجم السلطان السيبراني الذي تتمتع به هذه المجاميع داخل حدود فضاء الفيض السيبراني المحلي والعولمي على حد سواء.

3. 1. 1. مجموعة *Ashiyane*[131]:

تستقر هذه المجموعة من قراصنة المعلومات، وبجدارة، بالمرتبة الأولى بين بقية مجاميع القرصنة المقيمة في مجتمع القرصنة السيبرانية بإيران. وقد استحقت هذا المقام المتميز لأسباب عدة، منها: إدارتها لمؤسسة تجارية تعنى بمعالجات وحلول أمن المعلومات، وأخرى اطلقت عليها مجموعة فريق *Ashiyane* للأمن السيبراني *Digital Security Team* والتي تقوم بإعداد وتدريب وترخيص كوادر وطنية للقرصنة المشروعة (قراصنة ذوي القبعات البيض)، كما أنها تنهض بمهمة تشغيل وإدارة منتدى يحتضن الجهابذة، والجيل الصاعد من قراصنة المعلومات الإيرانيين، فيجيب عن استفساراتهم، ويوجه مسارات نقاشاتهم البرمجية، كما ويوفر لهم بالوقت ذاته دعماً تقنياً لتطوير مهاراتهم وترسيخ خبراتهم، أو يسعى الى تجنيدهم في إحدى المؤسسات الحكومية التي تسعى لجذب المتميزين الى فصائلها السيبرانية[132] (*Azani,2015*).

وقد أضافت شخصية إدارة هذه المجموعة[133]، بيروز كماليان، المزيد من الأضواء على هذه المجموعة نظراً لما يتمتع به من مكانة مرموقة في مجتمع المعلومات الإيراني وعلى الساحة السياسية بالوقت ذاته، كما أن اسمه قد أدرج على قائمة المنع والملاحقة في دول الاتحاد الأوربي، نتيجة لاتهامه بممارسات تتعارض مع مبادئ حقوق الانسان، وذلك بسبب مشاركته ودعمه للأجهزة الأمنية في توفير معلومات عن هوية المشاركين بالانتفاضة الخضراء، مما أسهم في مداهمة المعارضة الإيرانية خلال الانتخابات الرئاسية عام 2009 وإلقاء القبض على كثير منهم بواسطة شرطة فضاء إيران السيبراني *FATA*.

إلا أن هذه المقاطعة، ومناهضة كماليان للإدارة الأمريكية، لم تمنع الشركات السيبرانية الأمريكية من التعامل مع مواقع المجموعة ومنتدياتها، فقد استضيفت في خادم لشركة أمريكية بولاية اوهايو، مع مجموعة مواقع أخرى تعود ملكيتها وتدار بواسطته (*Kagan&Stiansen,2015*).

وضع كماليان الحجر الأساس للمجموعة عام 2002 ليحقق غاية أساسية نشبت في دخيلة نفسه للارتقاء بالحصانة الأمنية لمواقع الويب الإيرانية، ثم أضاف الى قائمة غاياته من تأسيس المجموعة مناهضة الولايات المتحدة وسياساتها المعادية لإيران من خلال ممارسة سلسلة من عمليات القرصنة على مواقعها الحساسة.

في البداية كانت المجموعة تمارس القرصنة بجميع الاتجاهات، ودون أن تتبنى أي نهج يحمل في طياته انتماءَ محدداً لجهة معينة، شأن الكثير من مجاميع القرصنة المنتشرة في فضاء الفيض العولمي. فحملت بعض هجماتها (في أول

131 . كلمة *Ashiyane* تستخدم في اللغة الفارسية وتطلق على العش أو الوكر الذي تلجأ اليه وتقيم فيه الطيور وصغارها، من أجل ذلك نلاحظ كثرة استخدام اصطلاحات صغار الطيور وأفراخها في كثير من خطابات التواصل بين أعضاء هذه المجموعة.

132 . كان موقع المجموعة *Ashiyane.org* حاضراً في فضاء الانترنيت منذ عام 2003، وقد تكاثر عدد زواره نتيجة للمواد الخصبة المطروحة في أقسامه المتعددة، حيث بلغت مرتبته بحسب احصائيات موقع *Alexa* مرتبة متقدمة بعد أن بلغ عدد الزيارات للموقع حوالي 900,000 زيارة يومياً، وبلغ عدد الزائرين المنفردين 130,000 زائر يومياً، وبمتوسط 6.9 مراجعة للمحتوى للزائر الواحد (*HP,2014*).

133 . تألفت المجموعة في بداياتها من ثلاثة أعضاء هم: بيروز كماليان (واختار لنفسه اسم *aka Behrooz_Ice*)، ونعمة صالحي (واختار لنفسه اسم *aka X7Q*)، وعلي رضا شيرازي (واختار لنفسه اسم *aka ActionSpider*) وقد توزعت المهام بين الأعضاء الثلاثة، فاتفقوا على تسليم قيادة المجموعة لبيروز كماليان، فأصبح الواجهة الإعلامية للمجموعة، بينما أوكلت لصالحي مهمة إلقاء المحاضرات وحضور الندوات حول القرصنة السيبرانية، إضافة الى إدارة موقع المجموعة. أما علي شيرازي فكان مسؤولاً عن مهاجمة وتدمير مواقع الويب المناوئة لنهج المجموعة.

الأمر) صبغة وطنية صرفه بمناهضة رقمية لأعداء الأمة الإيرانية، عندما قامت بسلسلة من هجمات القرصنة الناجحة على مواقع متعددة تعود الى وكالة الفضاء الأمريكية في منتدى القرصنة العالمي *Zone-h(.)org* في خطوة مباشرة لمناهضة الحملة الإعلامية الشرسة التي قام بها الرئيس الأمريكي السابق ضد إيران. كما لم تنجو المواقع الإيرانية الحكومية من هجمات المجموعة، فقام بعض أعضائها بأكثر من هجمة على مواقع حكومية بالبلاد منها موقع جامعة شريف للتقنية عام 2008 (*Kagan&Stiansen,2015*).

بيد أن ثمة تحول جذري قد حصل بسياسة كماليان في قيادة المجموعة عندما بدأت الانتفاضة الخضراء التي ناهضت ما صاحب حملة انتخاب رئيس البلاد عام 2009، من انتهاكات، فتوجه قائد المجموعة بكليته، مع أعضاء المجموعة باتجاه النظام الإيراني، بعد أن لاحظ الدعم غير المسبوق الذي وفرته الإدارة الأمريكية للمعارضة الإيرانية، وتسخير مواقع التواصل الاجتماعي لتأجيج ثورة جديدة تعصف بإيران، فاتخذ قراره بالانتماء الى معسكر النظام وبدأ بالتوجه نحو تسخير طاقات مجموعته، وتوجيه أدوات القرصنة نحو المعارضة والجهات الداعمة لأنشطتها فأصبحت المجموعة لصيقة بخطاطة النظام وقياداته المحافظة منذ لك الوقت.

وقد دشّن كماليان التعاون مع الإدارة الحكومية عندما قام بنشر صور حزمة كبيرة من البيانات التي تخص صور وهوية المعارضة السيبرانية التي تأجج نشاطها أثناء الحملة الانتخابية، مما ساعد أفراد شرطة إيران السيبرانية *FATA* في تتبع آثار حضورهم السيبراني، وأعان هذه القوات في إلقاء القبض عليهم بعيد انتهاء الإضرابات وإيداعهم في قبضة المحاكم الإيرانية.

ولم تمر سوى سنتين على الانتفاضة الإيرانية، وشروع المجموعة بالتعاون مع مؤسسات النظام الإيراني، حتى هرع كماليان الى تأسيس ومجموعة فريق *Ashiyane* للأمن السيبراني *Digital Security Team* التي استبطنت جملة من الأنشطة التي تضمنت قرصنة مواقع التيارات المناهضة والاصلاحية بالبلاد، كما لم تسلم من هجمات القرصنة الكثير من المؤسسات الدولية التي تدعم الناشطين وتدعو الى رعاية حقوق الانسان فكانت هذه الهجمات سبباً في إدراج الاتحاد الأوربي لاسم قائد المجموعة على قائمة الحظر الطويلة الموجودة لديه في عام 2011.

في البداية، توجه اهتمام المجموعة نحو ترسيخ الوعي بمسائل الأمن والحصانة السيبرانية تجاه مختلف أشكال التهديدات. وقامت بطرح محتوى علمي وتقني بالمجان على صفحات الويب لموقعها حول كيفية الكشف عن الثغرات الأمنية، والتعامل معها وكيفية الارتقاء بالحصانة الأمنية لمواقع الانترنيت في إيران. ثم تحولت بعد بضعة سنوات فتوجهت نحو الدخول الى سوق المعلومات عبر بوابة سياسات وتطبيقات أمن المعلومات، وبعدها أنشأت منتدى لاحتضان ورعاية وتوفير المشورة للعاملين في مجال الأمن السيبراني، والقرصنة السيبرانية، التحق به بضعة آلاف من الأعضاء الذين ينتمون الى الفضاء السيبراني الإيراني (*ICT,2014*).

وبدأت المجموعة بترسيخ حضورها في فضاء القرصنة العولمي، حتى بلغت مرتبة متقدمة بين مجاميع القرصنة العولمية بناء على التقييم الذي أصدره موقع القرصنة الشهير *Zone-H.org* والتقرير الصادر عن مركز حروب فضاء الفيض السيبراني[134].

[134] .كذلك احتلت المجموعة المرتبة الثانية بين مجاميع القرصنة في الفضاء السيبراني العولمي بناء على تقرير مركز حروب فضاء الفيض السيبراني الصادر في النصف الثاني من عام 2012، بعد أن أظهرت الإحصائية أن عدد الهجمات التي قامت بها المجموعة خلال عام 2012، قد بلغت 5799 هجمة، توزعت بين 2531 هجمة فردية، و3268 هجمة مشتركة (*Martin,2012*).

تطورت مجموعة *Ashiyane* خلال عقد من الزمن، وبعد أن التحقت بها مجموعة من قراصنة المعلومات المحليين، فبلغ عدد أفراد المجموعة أربعين عضواً، وتوطدت الجسور التي ربطتها مع النظام الإيراني، وانبسط سلطانها على أكثر من نشاط تجاري ارتبط بملفات أمن المعلومات وحماية المواقع الالكترونية في عموم الفضاء السيبراني الإيراني. وأصبحت تمتلك بوابة رقمية لتدريب قراصنة المعلومات وتجنيد الطاقات الشابة التي تمتلك مواهب واعدة[135].

من جهة أخرى، فقد مارس منتدى المجموعة دوراً مهماً في لمّ شمل قراصنة المعلومات، داخل حدود سلطانها، وخارجه، مع تنظيم حضورهم وممارساتهم داخل المنتدى وخارجه. من اجل هذا اولت إدارة المجموعة اهتماماً خاصاً في تشكيل معمارية تنظيمية تشابه الى حد كبير معمارية الوحدات العسكرية، حيث تلعب عدد سنوات الخدمة دوراً مهماً في تقديم القرين على بقية أقرانه، مع منحه صلاحيات أكبر، وفرض طاعته على من هم أصغر منه سنّاً، وأقلّ منه دراية ومعرفة.

ونلاحظ في تراتبية المجموعة أن الأعضاء النظاميين الذين يتقلدون مناصباً في إدارة النظام، والمنتدى، وإدارة الموارد البشرية، تقع أعمارهم في نهاية عقد العشرينات، اما أعضاء العش[136] النشطين فتتراوح أعمارهم بين 16-23 عاماً. ويلتزم الأعضاء القدامى بتدريب الأعضاء الجدد وإبداء المشورة لهم، وتوفير الدعم الذي يذلل أمامهم الصعاب في سبيل ممارسة القرصنة السيبرانية[137].

وقد ذهب الكثير من المتخصصين في مجال القرصنة السيبرانية الى تأكيد العلاقة الوثيقة بين هذه المجموعة ومؤسسة الحرس الثوري الإيراني بعد أن تأكد لديهم أن الكثير من الأنشطة التي تمارسها ليست إلا تنفيذاً لخطاطة النظام وتوجهاته التي تنقل إليها بواسطة قيادات المؤسسة. بينما ذهب آخرون الى أن تنظيمات القرصنة الحكومية تتلقى الأوامر والتوجيهات من المجموعة ذاتها، أو أنها قد التحقت بتنظيمات الحرس الثوري الإيراني فأصبحت جزءاً من قسم الالفضاء السيبرانيي الملتحق بالمؤسسة ذاتها (*IDC,2013*).

من أجل هذا فإن الإدارة الحكومية في إيران قد غضت الطرف عن أفراد هذه المجموعة وسمحت لهم باستخدام مواقع التواصل الاجتماعي، ومنحتهم فرصة الدخول المناطق المحظورة على الغير في فضاء الانترنيت، مع عدم وجود ملاحقة لهم من قبل كوادر شرطة الفضاء السيبراني الايراني، وذلك بسبب الخدمات المميزة التي يقدمونها للنظام في مجال القرصنة السيبرانية، ومهاجمة مواقع خصوم النظام داخل إيران وخارجها (*HP,2014*).

وتستضاف مواقع مجموعة *Ashiyane* وبنيتها التحتية السيبرانية (التي تتألف من صفحتها الرئيسة، ومنتدى المجموعة، وبوابة التدريب، ومواقع رفع الملفات، وموقع مجلتها الالكترونية) لدى مضيفات خدمة بالولايات المتحدة (شركة *Cloud Flare Inc.* في سان فرانسيسكو، وشركة *XLHost*)، كما أن المجموعة قد توجهت بالوقت ذاته الى مضيفات في المانيا (شركة *Hetzner AG*) (*Kagan&Stiansen,2015*).

3. 1. 2. مجموعة *Ajax Security Team*:

أنشئ فريق *Ajax Security Team* عام 2010 على يد اثنين من قراصنة المعلومات الإيرانيين أحدهما أفصح عن اسمه الحقيقي وهو علي علي بور (أطلق على نفسه اسم *aka Cair3x*)، أما الثاني فلا نعلم عنه سوى اسمه في مجال

---

135 . تؤكد الكثير من التقارير والدراسات على أن بوابة التدريب التي تعود الى هذه المجموعة تقوم بتدريب قراصنة المعلومات الذين يعملون بمعية الفصائل السيبرانية للحرس الثوري الإيراني، ومؤسسة الباسيج.

136 . سبق وأن ذكرنا أن معنى *Ashiyane* تعني باللغة الفارسية عشّ الطير أو وكره.

137 . ويتمتع جلّ أعضاء المجموعة النظاميين بمستوى مرموق من التعليم الجامعي، مضافاً اليه خبرات والمهارات التي تطوّرت نتيجة للالتحاق بدورات تدريبية متعددة، بالإضافة الى الممارسات الميدانية التي استرشدت بتوجيهات خبراء في قرصنة المعلومات.

القرصنة وهو *HUrr!c4nE!* ودوون أن تتوفر لدينا معلومات عن اسمه الحقيقي. تخصص هذين القرصانين بممارسة الهجمات على مواقع الويب بعد أن تتلمذا وتلقنّا علوم القرصنة، ومهاراتها، نتيجة لانتمائهما لكل من منتدى مجموعة *Ashiyane* ومنتدى مجموعة *Shabgard* (*Villeneuve,et.al.,2013*).

ورغم عدم تصريح الشخص الثاني، (المؤسس للمجموعة عن هويته الحقيقية) واختفائه وراء اسم رمزي، فإنه بالمقابل يعد الأكثر حضوراً من بين أعضاء المجموعة في فضاء الانترنيت، مع قيامه

بتسجيل اسم نطاق منتدى المجموعة *ajaxtm[.]org* بواسطة عنوان بريده الالكتروني، إضافة الى موقع *aerospace2014[.]org* الذي يستخدم في التجسس على مواقع ويب بالولايات المتحدة الأمريكية، وتتبع المستخدمين الإيرانيين الذين يوظفون أدوات القفز فوق نظم الرقابة والحظر التي توظفها الإدارة الحكومية في فضاء الانترنيت في إيران.

وقد التحق بالقرصانين المؤسسين قراصنة آخرون مثل: "*Crim3r*" & "*Mohammad PK*", "*0day*"قبل أن تتوجه المجموعة نحو إنشاء منتدى للقراصنة حمل اسمها *ajaxtm[.]org* والذي تزايد عديد الأعضاء المنتمين اليه فتجاوز عددهم على 236 قرصاناً (*Villeneuve,et.al.,2013*).

شأن بقية مجاميع القرصنة السيبرانية في إيران فإن هذه المجموعة قد أعلنت عن حضورها في البداية، بوصفها شركة متخصصة في أمن المعلومات وحماية وتطوير حصانة شبكات المعلومات لكل من القطاع الحكومي والقطاع الخاص[138]. كما أن الشركة قد عمدت الى طرح حزمة من البرامج التدريبية والتطويرية لمن يروم تطوير مهاراته في مجال اكتشاف الثغرات الأمنية في شبكات المعلومات وكيفية الارتقاء بالحصانة الأمنية (*IDC,2014*).

في البداية كانت عملية القرصنة بالنسبة لهذه المجموعة عبارة عن ممارسة تستعرض فيها قدرات أعضاء الفريق ومهاراتهم في عمليات الاختراق، وترسيخاً لمكانتهم التي يمكن أن تستثمرها على صعيد أنشطة معالجات أمن المعلومات في القطاع التجاري بالبلاد (*LeClaire 2015*). بيد أن أنشطتها قد تحوّلت تدريجياً باتجاه موالاة النظام ودعم آلته السياسية، فاشترك أعضاؤها في عمليتين ضد أعداء النظام هما "*#OpUSA* *and* "*#OpIsrael*" واللتين وجهتا حممها السيبرانية ضد مواقع إسرائيلية وأخرى أمريكية رداً على العملية الآثمة التي مارستها إسرائيل ضد قطاع غزة عام 2013. كما أنها مارست هجمات أخرى على مواقع المعارضة الإيرانية داخل حدود إيران، وأسهمت في تعطيل عمل هذه المواقع، ومارست عملية تشويه مادة المحتوى السيبراني المطروح على صفحات الويب، أو غيّرت مسار الزوار نحو مواقع أخرى مزيفة، بالإضافة الى الكشف عن هوية المستخدمين الذين يتجاوزون عقبة الجدار الأمني الذي أقامته مؤسسات أمن المعلومات في البلاد لحضر وصول المستخدمين الى مواقع معارضة على الانترنيت (*Villeneuve,et.al.,2013*).

لم يستمر حضور هذه المجموعة في مجتمع قراصنة المعلومات الإيرانيين (لمدة طويلة) فقد أشارت التقارير الى تضاءل الدور الذي تمارسه هذه المجموعة مع بدايات عام 2014، مع عدم وجود أي ادلة عن قيام أعضائها بهجمات ضد مواقع الويب منذ نهاية عام 2013، كما أن منتدى القراصنة الذي حمل اسمها والذي ادار أنشطته الرجل الثاني بالمجموعة *HUrr!c4nE!* قد توقف عن بث مشاركات جديدة، ثم توقف عن العمل نهائياً. وقد ربطت هذه الأمور بتحوّل المجموعة نحو مجال التجسس السيبراني على مواقع المعارضة الإيرانية، وتجاوز المستخدمين الإيرانيين على

---

[138] . اسم الشركة في سوق أمن المعلومات الإيراني هو شركة *Pars Pardazesh Hafez Shiraz Ltd.* المحدودة.

نظم المراقبة والحظر السيبراني، والتوجه نحو التجسس وجمع بيانات مهمة من مواقع خصوم الدولة وأعدائها خارج حدود الفضاء السيبراني الإيراني (*Villeneuve,et.al.,2013*).

3. 1. 3. مجموعة *Shabgard*:

أبصرت مجموعة *Shabgard* (التي تعني حارس الظل) النور في مجتمع قراصنة المعلومات الإيرانيين في شهر أغسطس من عام 2003 على يد محمد جورجاندي (الذي أطلق على نفسه اسم: s7az2mm)، وفي نفس العام الذي شهد ولادة مجموعة *Ashiyane* الشهيرة. وامتلكت شأن بقية المجاميع منتدى يحتضن قراصنة المعلومات في إيران، والذين بلغ عدد الذين سجلوا منهم في عضويته حوالي 13,549 عضواً[139]، كما حرصت على فتح بوابة لتدريب المستخدمين وبالتنسيق مع جامعة بهشتي[140] للذين يرومون تحصين أنفسهم بخبرات القرصنة السيبرانية، والكشف عن الثغرات المقيمة في شبكات المعلومات (*HP,2014*).

وتلتحق هذه المجموعة بمجاميع قراصنة المعلومات التي تنسّق أنشطتها مع الإدارات الحكومية، وتوجه مسارات أنشطة قراصنتها بحيث تتناغم مع غايات النظام الإيراني وتوجهاته (*Connell,2014*). بيد أنه لا تتوفر معلومات دقيقة عن طبيعة هذا التعاون، كما أن حرص أعضاء هذه المجموعة على عدم الإفصاح عن عمليات الاختراق وقرصنة المواقع ضمن القنوات العامة (رغم عراقة مجموعتهم وحضورها بمضمار القرصنة السيبرانية في إيران منذ أكثر من عقد من الزمان) يضفي المزيد من الغموض عن طبيعة الدور الذي تمارسه المجموعة ضمن استراتيجية النظام الإيراني في درء المخاطر عن الفضاء السيبراني المحلي[141]، أو مباشرة هجمات على أهداف منتخبة لدى خصومها (*Manshrof,2013*).

ورغم ولادة هذه المجموعة خلال نفس الحقبة التي ولدت فيها مجموعة *Ashiyane*، إلا أنها لم تستطع تحقيق إنجازات كبيرة ترقى بها الى مستوى الثانية. من اجل هذا فقد صنفت بالمرتبة الثانية على مستوى مجاميع القرصنة المتحالفة مع النظام الإيراني (*Mansharof,2013*).

3. 1. 4. مجموعة *Mortal Combat*

تلتحق بمجاميع القرصنة الايرانية مجموعة *Mortal Combat* والتي تطلق على نفسها اسم *Underground Security Team* (*ICT,2014*). بدأت هذه المجموعة عملها منذ بضعة سنوات. بيد أنها تختلف عن بقية المجاميع بحرصها على عدم الإفصاح عن حضورها في وسائل الاعلام، كما أنها لم تسعى الى العمل تحت مظلة إحدى مسميات الشركات الأمنية في إيران. غير أنها قد حرصت على إنشاء موقع ويب يضم منتدى نشطاً، قد حصرت بعض محاوره بأعضاء المجموعة بعيداً عن أنظار بقية زوار الموقع (*Azani,2015*).

ورغم عدم إفصاح مجموعة *Mortal Combat* عن أنشطتها إلا ان الشكوك تحوم حول مسؤوليتها عن صناعة الفايروس الذي هاجم بضعة مواقع إسرائيلية في صيف عام 2012 وأطلق عليه (في حينها) اسم فايروس الامام المهدي *Mahdi Virus* (*Azani,2015*).

---

[139] . رغم مرور أكثر من عشرة أعوام على افتتاح موقع المنتدى فقد توقف عن العمل مع بدايات عام 2014، دون الإعلان عن سبب هذا التوقف المفاجئ (*HP,2015*).

[140] . تشمل برامج التدريب التي تطرحها مجموعة Shabgard على موقعها: حزمة من البرامج التدريبية التي تنمي مهارات اختراق المواقع، وكيفية استخدام تطبيقات أمن الشبكات، ومكافحة البرمجيات الضارة، ودرء الهجمات السيبرانية. وتقوم البوابة بمنح شهادات ترخيص للمشاركين وبالتنسيق مع جامعات إيرانية مرموقة.

[141] . من جهة أخرى أشارت تقارير معهد الأبحاث الإسرائيلي *INSS* الى أن مجموعة *Shabgard* ترتبط مع مؤسسة الحرس الثوري الإيراني، إلا أن طبيعة العلاقة التي تجمع بينهما لا زالت غير واضحة.

3. 1. 5. مجموعة *IT Security Team*:

تعد مجموعة *ITSec Team* من مجاميع القرصنة السيبرانية المرموقة في إيران، والتي عملت ضمن شركات أمن المعلومات المنتشرة في البلاد بكثافة، وامتلكت موقع ويب نشط، بيد أن هذا الموقع كان خالياً من اية إشارة الى عديد أعضاء المجموعة أو هويتهم (*Azani,2015*). غير أن ما يميز هذه المجموعة هو نجاح مساعيها في إنتاج وتوزيع الكثير من أدوات الكشف عن مواطن الثغرات السيبرانية المقيمة في النسيج الشبكاتي، وأخرى لممارسة عمليات القرصنة السيبرانية[142]. وتعمل هاتين الأداتين سوية، حيث تقوم الأداة الأولى *Web Application Exploiter* بالتنقيب عن الثغرات السيبرانية المقيمة في تطبيقات النسيج الشبكاتي، بينما تباشر الأداة الثانية (والتي أطلق عليها اسم حزمة الجزرة *Havij Tool*) بحقن أداة قرصنة من نوع *SQL Injection* بصورة آلية لممارسة عملية قرصنة الموقع (*ICT,2014*).

3. 1. 6. مجموعة *Iran Hackers Sabotage Team* :

أنشئت المجموعة عام 2004 واضعة نصب أعين مؤسسيها ضرورة إدراج اسم إيران ضمن مرتبة متقدمة على صعيد تقنية القرصنة والأمن السيبراني. تعد هذه المجموعة من مجاميع القرصنة النشطة في إيران، وتحتل مكانة متقدمة بين فرق القرصنة المتميزة ضمن موقع *Zone-H.org* بوصفها من المجاميع التي يكثر عديد هجماتها على مواقع ويب تعود الى مؤسسات حكومية، وشركات تجارية، ومؤسسات أكاديمية بالولايات المتحدة الأمريكية. وقد اشارت الإحصائية المسجلة في موقع *Zone-H.org* الى ان المجموعة قد شنّت خلال عام واحد 3551 هجمة، مورست 481 هجمة منها بصورة فردية، بينما بلغ عدد الهجمات الشاملة منها 3069 هجمة (*ICIT,2015*).

وبعد أن بسطت المجموعة سلطانها على صعيد القرصنة السيبرانية، وأثبتت جدارتها بين مجاميع القرصنة على المستوى العولمي، وبلغت آثار هجماتها مواقع لدول متقدمة، توجهت شان بقية مجاميع القرصنة بإيران نحو تأسيس شركة تجارية تعنى بتقديم خدمات أمن المعلومات وحماية مواقع الويب، وتدريب الكوادر الوطنية.

ورغم توسع دائرة أنشطة القرصنة التي تمارسها هذه المجموعة، إلا أن عدد أعضائها لم يتجاوز ثلاثة أعضاء أطلقوا على أنفسهم أسماء مستعارة هي: *NT,C0d3r & Lord* وقد أفصح الأول والثاني عن كونهما طالبين في إحدى الجامعات الإيرانية، أما الثالث فيدّعي أنه باحث في مجال أمن المعلومات والبرمجة دون أن يفصح عن مكان عمله (*ICIT,2015*).

3. 1. 7. مجموعة الامبراطور *Emperor Team*:

تعد من مجموعات القراصنة ذوي القبعات السوداء، ممن يسخرون أنشطتهم لممارسات غير معلنة مقابل الظفر بمردود اقتصادي مباشر، أو غير مباشر. بدأت نشاطها عام 2001 على يد قرصان المعلومات أمير حسين سيرافي، والذي بدأ بمهاجمة مجموعة من مواقع الويب، ثم توجه الى ممارسة هجمات على مواقع ملحقة بموقعي *MSN & Yahoo*.
وبدأ القراصنة المحليون بالالتحاق في هذه المجموعة، فأنشأوا موقعاً أطلقوا عليه اسم موقع الايمان *Iman Online*.
بعدئذ توجهت اهتماماتهم نحو تصنيع أدوات قرصنة يسهل استخدامها، مثل: *Mail Bomber, Port Scanner*
وكانت غاية المجموعة الظفر بالشهرة بين قراصنة المعلومات المحليين، وإدراج أنشطتهم على موقع *H.org* (*IDC,2014*).

---

142 . أشار الباحث (*Azani,2015*) الى أن الذين قاموا بتصنيع هذه الأدوات من أعضاء الفريق هم: فارشاد شاهبازي (aka r3dm0v3)، وأمين شوكوهي (aka Pejvak) وبالتعاون مع عضوين آخرين من المجموعة هما: يشار شاهين زاده وبهزاد رافان بخش.

وبعد أن طارت شهرتهم في مجتمع قراصنة المعلومات الإيراني، أتيحت لهم أكثر من فرصة لتوظيف مهاراتهم بصورة احترافية، وكانت الفرصة الأولى عبارة عن دعوة من إحدى الشركات الإيرانية بممارسة هجمة معلوماتية على إحدى قواعد بيانات المؤسسات الحكومية بقصد استراق المعلومات الموجودة على خادم الشركة. ثم تزايد الطلب على خدماتهم، فمارست المجموعة سلسلة هجمات على مواقع اثنين من المرشحين للانتخابات الرئاسية عام 2005 (*IDC,2014*).

3. 1. 8. مجموعة *Tarh Andishan*:

بعد أن أعادت الإدارة الحكومية الإيرانية حساباتها بصدد تخصيص الموارد المالية المطلوبة لتطوير الحصانة الأمنية للبنى التحتية للمعلومات والاتصالات في إيران، فضاعفت التخصيصات المالية الى عدة اضعاف، جاءت ولادة مجموعة[143] *Tarh Andishan* تعبيراً عن رغبة الإدارة الحكومية في صياغة استراتيجية جديدة تهدف الى توفير قوة رقمية ضاربة للرد على الهجمات السيبرانية الشرسة التي تكاثرت أعدادها وتعددت أهدافها في أجزاء حيوية من الفضاء السيبراني الإيراني بواسطة البرمجيات الخبيثة *Stuxnet, Duqu & Flame* فبلغت آثارها الضارة أجزاء واسعة من منشآت الطاقة الذرية الإيرانية، ومنشآت إيرانية أخرى خلال السنوات 2009-2012 (*ICIT,2015*).

بلغ عدد أعضاء المجموعة 20 عضواً ممن يمتلكون خبرة ومهارات متميزة على صعيد القرصنة السيبرانية وتطوير البيئات البرمجية، يقيم معظمهم في العاصمة طهران. ويلتحق بأنشطة هذه المجموعة ثلّة من قراصنة المعلومات الإيرانيين ممن يقيمون في كندا، وبريطانيا، وهولندا، وينسقون أنشطتهم مع أعضاء المجموعة الذين يقيمون في العاصمة طهران (*LeClaire,2015*).

وتعتمد المجموعة (في تسيير دقة أنشطة قرصنتها السيبرانية)على برمجيات قادرة على التوالد الذاتي Self-Propagating Software تدعمها مجموعة من النظم البرمجية المتطورة والتقنيات الأمنية مثل: البوابات الخلفية Backdoors، وأدوات حقن SQLالبرمجيات الخبيثة (O'Connell,2015).

ويستضاف موقع المجموعة وبنيتها التحتية (داخل حدود الفضاء السيبراني الإيراني) لدى كل من مجهز الخدمة المحلي (*Netafraz.com*)، ونظم شبكات المعلومات *Autonomous System Networks* (*ASNs*). كما أن المجموعة قد سجلت حضورها السيبراني ضمن نظام النطاق الإيراني *DNS*، وهوية الحضور عبر نظام *IP Source Net-Blocks* واللذان يؤشران بجلاء الى وجود ارتباط عميق بين شبكة المجموعة وشبكات نفط وغاز إيرانية تمتلك موارد بشرية ذات خبرة عميقة بنظم إدارة شبكات المعلومات الصناعية *ICS Systems* (*ICIT,2015*).

وقد أعلنت المجموعة أكثر من مرة عن رغبة اعضائها بالتحكم في نظم إدارة صفحات الويب المنتشرة في فضاء الفيض السيبراني ـ العولمي، في إشارة الى امتلاكهم سلطاناً رقمياً غير مسبوق بالمقارنة مع بقية مجاميع القرصنة الموجود في إيران، ودول المنطقة (*O'Connell,2015*).

وقد أكدت الدراسة التي أصدرتها مؤسسة *Cylance* (إحدى المؤسسات الأمريكية التي تعنى بمسائل أمن معلومات فضاء الفيض السيبراني) عام 2014 حول نتائج تحليل الهجمة السيبرانية واسعة النطاق، والتي أطلق عليها *Operation Cleaver* على وجود هذه الغاية بعد أن كشفت اللثام عن قيام هذه المجموعة بأخطر هجمة معلوماتية (لـ غاية هذا التاريخ) استهدفت أكثر من خمسين كياناً مؤسسياً ـ حيوياً (شملت مؤسسات عسكرية، وشركات نفط

[143] . تطلق عبارة *Tarh Andishan* باللغة الفارسية على المتميزين من المفكرين والمبتكرين.

وغاز، ونظم توليد وتوزيع الطاقة الكهربائية، ومنظومات نقل، وخطوط جوية، ومطارات، وموانئ، ومؤسسات صناعية متقدمة) تعود الى أكثر من 16 بلداً في الوقت ذاته.

ولعل من أهم الاستنتاجات التي توصلت اليها هذه الدراسة، (والتي استغرقت سنتين من التحقيقات والتحليلات المضنية) أن قيام مجموعة *Tarh Andishan* بهذه الهجمات الواسعة يؤشر بجلاء الى أن هذه المجموعة تهيمن على إدارة بنية تحتية واسعة النطاق، وتوظف تقنيات اختراق، وتحليل نظم أمن شبكات المعلومات يعزّ توفرها لدى ثلّة من قراصنة المعلومات، أو مجموعة من مجاميع القرصنة. الأمر الذي أكد وجود دعم على مستوى عال لا يمكن أن يتوفر الا بظل دعم حكومي سخي (*LeClaire,2015*).

إن السيناريو بالمعقد، الذي انصبغت به تفاصيل عملية *Operation Cleaver* وطبيعة، وحجم الأهداف التي استهدفتها العملية، وتعدد البلدان التي شملها هذا السيناريو الذكي، يعد مؤشراً على ولادة مجموعة قرصنة تمتلك قدرات غير مسبوقة في ممارسة سلسلة من الهجمات التدميرية التي يمكن أن تمتد تأثيراتها الضارة على عموم فضاء الانترنيت العولمي (*Holler,2015*).

وإذا كانت ولادة الفايروس *Stuxnet* بداية لعهد جديد من البرمجيات الخبيثة التي تمتلك القدرة على التأثير في اهداف منتخبة، فإن عملية *Operation Cleaver* يمكن أن تعد مؤشراً على ولادة مجاميع قرصنة (تعد مجموعة *Tarh Andishan* واحدة منها) تمتلك سطوة رقمية غاشمة، يمكن أن تسخّر لإحداث أضرار شاملة ستصاب بآفاتها أجزاء واسعة من النسيج الشبكاتي العولمي، مع حصول شلل في كثير من المؤسسات الحيوية، داخل حدود الفضاء المتخيّل، وخارجه بالوقت ذاته (*Nightingale,2015*).

ولا يمكن لمثل هذه السطوة السيبرانية أن تتوفر إلا لدى عدة فرق من القراصنة المتمرسين (يدار عملها بواسطة إدارة ذكية) يتكامل عملها في أكثر من مجال من مجالات الكشف عن الثغرات السيبرانية، وتحديد هوية وأهمية الأهداف المنتخبة، وتنسيق الهجمات، وتوظيف أدوات رقمية متطورة لممارسة هذه الهجمات، قادرة على التسلل من الجدران الـ نارية، والقفز من فوق نظم المراقبة الصارمة لكي تبلغ أهدافاً ليست تقليدية، ولتحقيق غايات غير معلن عنها، الأمر الذي يعمّق من خطورة الدور الذي يمكن أن تمارسه هذه المجموعة في المستقبل القريب (*Constantin,2014*).

بيد أن حضور هذه المجموعة وأنشطتها لم تستمر طويلاً في طهران، فقد حرمت منها مجاميع القراصنة بالإضافة الى حرمان العاملين في مجال أمن المعلومات المحليين عندما أقدمت السلطات المحلية على حضر أنشطة قرصنتها في شهر أبريل من عام 2006 دون أن تعلن عن أسباب ومبررات هذا الحظر (*Arquilla&Borer,2007*).

بالإضافة الى هذه المجـاميع هناك مجاميع أخرى يصعب حصرها من قراصنة المعلومات الإيرانيين، لم نحاول أن نعرّج عليهم خشية الاطالة ولأن منجزاتهم لا توازي ما أنجزته المجاميع التي انتخبناها واودعناها في هذه الفقرة[144].

---

[144] . فعلى سبيل المثال، لا الحصر، تعد مجموعة قراصنة إيران . المخربين *IHS Iran Hackers Sabotage* من المجاميع الإيرانية الرائدة في مجال قرصنة المعلومات، والتي بدأت بممارسة أنشطتها في بداية العقد الأول من الألفية الجديدة. وقد بررت ممارستها للقرصنة السيبرانية على مواقع الويب واختراق مضيفات الخدمة لإثبات أن لإيران قدم راسخ في مضمار الأمن السيبراني، أسوة بالدول الغربية الرائدة في هذا المضمار (*Arquilla&Borer,2007*). وبعد أن نجحت الكثير من الهجمات التي مارستها المجموعة في فضاء الانترنيت[144]، وتوفر القناعة الكافية لدى المجموعة برسوخ قدمهم في هذا المضمار وتحقيق رسالتها، توجهت نحو إنشاء شركة متخصصة بأمن المعلومات، تمارس دور الكشف عن الحصانة الأمنية لنظم المعلومات والنسيج الشبكاتي، مع تحديد مواطن التهديدات المحتملة، وإبداء المشورة لحماية الموارد السيبرانية التي تعود للقطاع الحكومي أو القطاع الخاص في إيران.

ورغم ذلك لا زالت مجاميع وفرق قراصنة المعلومات الإيرانيين تتبوأ (سواء المتحالف منهم مع النظام وغير المتحالفين معه) مراتب متقدمة ضمن تراتبية فرق القرصنة العولمية التي تستوطن الجزء المظلم من فضاء الفيض السيبراني[145].

فعلى صعيد أكثر عشرة مجاميع القرصنة، سيئة السمعة، على المستوى العولمي، احتلت مجموعة *Tarh Andishan* المرتبة السادسة (*O'Connell,2015*). أما على صعيد أكثر عشرة مجاميع في قطاع القرصنة السيبرانية، والتي تنال دعماً من حكوماتها، وتسعى الى نشر الخطاب السياسي للنظم الحاكمة، وينذر حضورها بالسوء نتيجة لهجماتها الشرسة، فقد احتلت المجموعة ذاتها المرتبة التاسعة، بينما احتلت مجموعة *Ajax Security Team* المرتبة السادسة (*LaClaire,2015*).

وقد أدرج على قائمة المطلوبين لمكتب التحقيقات الفدرالي بالولايات المتحدة الأمريكية لعام 2016، سبعة أسماء لقراصنة معلومات من إيران قد مارسوا سلسلة من الاختراقات، والهجمات الخطيرة على مواقع تخص مصارف أمريكية، كلفت الولايات المتحدة بضعة ملايين من الدولارات، إضافة الى مباشرة تهديد خطير لمنظومة الإدارة الالكترونية لسد مدينة نيويورك. وقد أثبتت التحريات أن هؤلاء القراصنة يعملون بمعية شركات أمنية تتلقى دعماً من الإدارة الحكومية الإيرانية. وتضمنت القائمة كل من: أحمد فتحي، وحامد فيروزي، وأمين شوكوهي، وصديق أحمد، وأوميد غفراني، وسينا قيصر، ونادر سعيدي (*Wei,2016*).

ولم تقتصر أنشطة القرصنة السيبرانية في إيران على الممارسات التي تقع ضمن قطاع القرصنة السوداء *Black Hacks*، أو القرصنة الرمادية التي تمارس في الجزء المظلم من مواقع الويب، ولكنها امتدت أيضاً الى الجزء المنير منه حيث يكثر القراصنة ذوي القبعات البيضاء لضمان توفير حصانة أمنية لالفضاء السيبراني الوطني. حيث يمكن ملاحظة تزايد أنشطة القرصنة البيضاء *White Hacks* التي يروم أصحابها سد الثغرات الأمنية والارتقاء بالحصانة الأمنية لنظم المعلومات والتطبيقات البرمجية لدرء مخاطر التهديدات والهجمات المحتملة التي يمارسها قراصنة معلومات من داخل إيران، أو خارجها.

وقد ترعرع هذا النمط من القرصنة الإيجابية في أروقة المعاهد والجامعات الإيرانية وعلى يد أساتذة وخبراء في أمن المعلومات لقّنوا طلبتهم كيفية الكشف عن مواطن الضعف في النسيج الشبكاتي، والافصاح عنها للجهات المعنية لغرض إحكام امنها وحمايتها من التهديدات والهجمات المحتملة. ولعل من أشهر فرق القرصنة البيضاء في إيران (*Patterson&Smith,2005*):

- فريق أمن القبعة الأمنية *Hat Squad Security Team*.
- فريق أمن إيران *Iran Security Team*.
- فريق إيران للاستجابة الأمنية الطارئة *IR Computer Emergency Response Team*.
- قاعدة بيانات الفايروسات في إيران *Iran Virus Database*.
- فريق *Crouz* لأمن المعلومات *Crouz Security Team*.

---

[145] . لوحظ ارتقاء الأنشطة التي مارسها قراصنة المعلومات في إيران، وحضورهم المعلن قبل أن يتركز اهتمام الإدارة الحكومية بمسائل امن المعلومات. ولعل من أهم هذه الأنشطة قيامهم بتأسيس مجموعة محلية للقرصنة بطهران تنتمي الى مجاميع *Defcon Groups*[145] التي تنتشر في معظم بلدان العالم منذ عام 2004. بيد أن حضور هذه المجموعة وأنشطتها لم تستمر طويلاً في طهران، فقد حرمت منها مجاميع القراصنة بالإضافة الى حرمان العاملين في مجال أمن المعلومات المحليين عندما أقدمت السلطات المحلية على حضرها في شهر أبريل من عام 2006 دون أن تعلن عن أسباب ومبررات هذا الحظر (*Arquilla&Borer,2007*).

وتوفر عمليات المسح والرصد الأمني التي تمارسها ، باستمرار، هذه الفرق معلومات مهمة عن الثغرات الأمنية وكيفية معالجتها، على صفحات مواقعها الناطقة باللغة الفارسية، كما تعد جهة إرشادية للشركات الإيرانية التي قد تخصصت في إنتاج النظم البرمجية، بما توفره من معلومات أمنية رصينة عن طبيعة الثغرات المقيمة في نظمها البرمجية، فتساعدها في تجاوزها ضمن إصداراتها اللاحقة.

3. 2. مطالع تحالف النظام الإيراني مع قراصنة المعلومات:

بدأت مطالع أنشطة القرصنة السيبرانية الاحترافية في الفضاء السيبراني الإيراني في عام 2000 ونجحت مجاميع القراصنة المحليين في ممارسة هجمات متعددة على عدد كبير من مواقع الويب المستوطنة في هذا الفضاء، ودون تمييز بين انتماء المواقع، سواء في القطاع الحكومي أو القطاع الخاص. وقد تباينت شدة هذه الهجمات وعمق التأثير المصاحب لها، بيد ان هذه التأثيرات لم ترقى الى إحداث تخريب شامل بالمواقع، واقتصرت على إحداث خلل جزئي، وتوقف جزئي لبعض ساعات قبل أن تنجح إدارة النظام في إعادة التشغيل واحتواء تأثير الهجمة.

وقد شرع قراصنة المعلومات بالتكتل في مجاميع توحدها الرؤية والغايات وبادروا في تأسيس مجاميع، حرصوا في البداية على كتمان هوية أفرادها، قبل أن تتوفر لديهم الفرصة بالتوجه نحو إنشاء شركات صغيرة أو متوسطة تعنى بتوفير خدمات الحصانة الأمنية لمواقع الويب ونظم المعلومات التي تمتلكها شركات القطاع الخاص، قبل أن يتوجهوا بعرض خدماتهم الأمنية على مؤسسات حكومية.

وقد انتبهت مؤسسة الحرس الثوري الإيراني الى بروز ظاهرة القرصنة السيبرانية في الفضاء السيبراني الإيراني، مع توفر مناخ مناسب لتوسع هذه الممارسات نتيجة لتزايد أعداد خريجي الجامعات المتخصصة في علوم الحاسب وتقنية المعلومات، مع تزايد نسبة البطالة، مما يشكل بيئة خصبة لتفاقم ظاهرة القرصنة السيبرانية في ظل الطوق الأمني الصارم الذي يفرضه النظام بالتضييق على مجال الفيض السيبراني، فتوجهت نحو جذب صفوة القراصنة وتجنيدهم للعمل معها للتخفيف من الضغوط المحتملة لتطور ممارساتهم على أمن المعلومات الوطني، من جهة، ولكسب قوة رقمية ضاربة تساهم في درء آثار الهجمات المتزايدة من خارج إيران، والبدء بمشروع طموح لتأسيس قوة رقمية ضاربة يمكن أن تطال أهدافاً حيوية وموجعة لدى خصومها التقليديين.

وبدأت مجموعة من الشركات الأمنية المختلطة بالولادة منذ عام 2005 تحت غطاء توفير الحماية الأمنية لشركات القطاع الحكومي والقطاع الخاص، وإعداد برامج تدريبية للكوادر المحلية، بينما تستبطن تحالفات وثيقة مع مؤسسات الحرس الثوري الإيراني، والباسيج، والدفاع السلبي تروم من خلالها تنفيذ تفاصيل استراتيجية بعيدة المدى لبناء جيش رقمي تتسع رقعة حضوره على مساحة واسعة من مجال فضاء الفيض السيبراني، وبعيداً عن أنظار خصوم البلاد وأعدائها المتربصين.

لقد استثمر النظام الإيراني ومؤسساته الأمنية والعسكرية سمة النضوج والتنوّع التي يتسم بها مجتمع قراصنة المعلومات الإيرانيين، وكونه من أكثر المجتمعات نشاطاً وتأثيراً على مستوى الفضاء السيبراني العولمي، مع تعدد اتجاهات أفراده، ووجود أكثر من عامل يربط لحمة أعضائه، في إنشاء دوافع مشتركة فرضتها الهوية الإيرانية، والانتماء العقدي في ترسيخ عدة مستويات من التعاون غير المعلن بين أفراد هذه التركيبة المجتمعاتية وبعض المؤسسات العسكرية والأمنية (مثل: الحرس الثوري الإيراني، ومؤسسة الباسيج) فعمّق تلاحم النسيج الاجتماعي الرابط بين أفراده، وجعل الكثير من أهدافهم تتخذ مسارات تنصبغ بصبغة قومية، أو عقدية، أو سياسية.

منذ عام 2012، بدأت الحقائق تتأكد يوماً بعد يوم، عن وجود تحالف غير معلن بين النظام الإيراني وقراصنة المعلومات ممن يعملون بصورة انفرادية، أو من خلال مجاميع قد انصبغت بصبغة شركات متخصصة بأمن المعلومات

وحماية النظم الشبكات. بيد أن هذا التحالف لم تتضح أبعاده لغاية هذا التاريخ نتيجة لتداول عناصر ملفاته بصورة سرية، وبعيداً عن أنظار الرأي العام ووسائل الاعلام الإيرانية (*SenseCy,2014*).

وقد سعت إيران الى تمويه عناصر المشهد الذي جمع بين هذه الأطراف من خلال إعلانها عن تشكيل فصائل وقوات رقمية، بعضها قد ارتبط بوزارة الدفاع، أو مؤسسة الحرس الثوري الإيراني، أو مؤسسة الباسيج، أو منظمة الدفاع السلبي، دون أن تفصح عن طبيعة وهوية هذه التشكيلات، كما قد حرصت بالوقت ذاته على السماح بإطلاق تصريحات متفرقة عن بعض القيادات والإدارات الحكومية لا تكاد توفر صورة واضحة المعالم عن طبيعة هذا التحالف الاستراتيجي.

بينما تركت المجال مفتوحاً أمام قراصنة المعلومات، سواء ممن عمل منهم بصورة انفرادية، أو ضمن مجاميع القرصنة التي تعمل وراء أسماء رمزية، أو مستعارة، أو تحت أسماء شركات متخصصة بالحصانة الأمنية تعمل داخل إيران، لبث سيل من الأخبار عن اختراقاتهم، وتهديداتهم المستمرة للكيانات السيبرانية في دول المنطقة، أو في الفضاء العولمي حيث تتناسل مواقع خصوم إيران، ودون الإشارة الى تحريض النظام أو دعمه المباشر لمثل هذه الهجمات، لكي تبقى برامج تطوير القدرات الهجومية لإيران بعيداً عن أنظار خصومها في المنطقة وبقية بلدان الأرض.

إلا أن مهادنة النظام الإيراني لطبقة الصفوة والموالين للنظام من قراصنة المعلومات لم يمنعها من التعامل بشدة مع من يمارسون عملية القرصنة خارج حدود الخطاطة التي تبنتها بالتعامل مع هذا النمط من الأنشطة السيبرانية.

إن عدم الإعلان بصورة مباشرة عن التحالفات القائمة بين المؤسسات الحكومية ومجاميع قراصنة المعلومات المتكاثرة في إيران، مع عدم وجود دلائل أكيدة لدى مراكز الدراسات الغربية حول طبيعة الائتلافات والسياسات المشتركة سيجعل الإدارة الحكومية في إيران بمنأى عن الاتهامات المباشرة بالإعداد أو تنفيذ هجمات معلوماتية على مواقع للدول المناهضة لسياساتها لحين توفر ادلة قاطعة تدعم توجيه أصابع الاتهام إليها(*Lewis,2014*).

بيد أن الحكومة الإيرانية لا زالت تكيل بمكيالين في التعامل مع كيانات ومجاميع القرصنة السيبرانية في البلاد، فتغضّ الطرف عمن يمارسون القرصنة في الأجزاء المظلمة من الفضاء السيبراني حيث تشنّ الهجمات على المواقع، وتتسلل المتحسسات للتجسس السيبراني، أو تشوه مادة المحتوى المطروح على مواقع الانترنيت، ما دامت تتوافق مع خطاطتها السياسية، بينما تعد محاولة البعض للقفز على نطاقات الحظر والمراقبة غير المبرّرة على مواقع التواصل الاجتماعي قرصنة تستحق العقاب الصارم. فقد ذكر أحد قادة الشرطة السيبرانية في إيران أنه قد تم اعتقال أكثر من مائة قرصان معلومات خلال شهر نوفمبر عام 2015 بسبب ممارستهم اختراق للحظر على تطبيق التراسل السيبراني *Telegram* من خلال إنشاء 50 مجموعة مغلقة للتواصل فيما بينهم بعيداً عن أعين أدوات المراقبة الحكومية (*TN,2015*).

4. هيكلة مؤسسات الدفاع وحروب المعلومات الإيرانية:

استقرت أهمية الدور الذي يمارسه الفضاء السيبراني، بجانبيه الإيجابي والسلبي، على حضور الثورة الإسلامية في إيران، وفرص نشر خطابها ودرء الخطاب المعارض له، في لباب قناعات قيادات النظام، وإدارات مؤسساته الحيوية، الأمر الذي يبرر حرص النظام الإيراني على تشكيل بنية مؤسسية، محكمة البنيان، ومتعددة الطبقات، وتتسم ببنية معقدة، وأوكل إليها مهمة مزاولة عمليات الدفاع عن البيضة السيبرانية لإيران، من الهجمات التي تمارسها أنظمة الدول المناوئة لإيران، ولكفّ ممارسات المعارضة في الداخل إضافة الى حملات الحروب اللينة التي تمارس من خارج البلاد، وشنّ الهجمات واستهداف موارد التهديدات التي يمارسها أعداء إيران على كياناتها السيبرانية، ولباب نسيجها الشبكاتي.

ولم تكن عملية ولادة هذه الكيانات المؤسسية دفعة واحدة، ولكنها مرّت بسلسلة من المخاضات التي فرضتها طبية التغيرات الحاصلة في أنماط حضور الفضاء السيبراني في إيران، وطبيعة نزعات الاستخدام لدى المواطن الإيراني، بالإضافة الى ما حفل به الشارع الإيراني من احداث عصفت بالمتغيرات السياسية، والاقتصادية، والاجتماعية بالبلاد خلال عقدين من الزمان.

وشأن برنامجها النووي (الذي لا زال الغموض يلفه من نواح كثيرة، ولم تفلح الدول الكبرى في كشف النقاب عن جميع تفاصيله التي لا زالت إيران تحتفظ بالكثير من خيوطها المتشابكة) حرصت إيران على إنشاء هيكلة لمؤسسات الدفاع وحروب المعلومات اتصفت بتعقيد كبير، مع تعدد طبقات إداراته، وتشابك العلاقات الرابطة بين فصائله، ووحداته الدفاعية والضاربة، بالإضافة الى نشر حضور هذه المؤسسات ضمن أكثر من بقعة، ضمن الإدارات الحكومية المدنية، والأمنية والعسكرية بحيث تورث خصومها السيبرانيين عقبة تتبع موارد هجماته المحتملة، أو بلوغ مستوى مقبول لتقدير حجم سلطانه السيبراني في الفضاء السيبراني الافتراضي.

لقد توغلت هيمنة النظام الإيراني، خلال العقود الثلاثة الأخيرة، فبلغ سلطانها الى أعماق سحيقة في منظومة إدارة ومراقبة نظم الاتصالات والمعلومات المحلية، كما أن تعدد مسارات تعاملها، مع مختلف قطاعات هذا النشاط، منذ دخول فضاء خدمات الإنترنيت الى البلاد، وتعدد أشكال الهيكلة المؤسساتية التي سعت الى تشكيلها، وتعدد المراجعات لبنية هذه المؤسسات، للتأكد من نجاح الاستراتيجية الأمنية، وارتفاع مستويات الحصانة، نتيجة الى السعي المستمر لتشتيت مراكز القوى، والمبالغة في تشبيك العلاقات الرابطة عن عناصر هذه المؤسسات، وتغييب دور الإدارات بشكل متعمد، الأمر الذي مهد للنظام فرصة إشراك عدد كبير من قطّان الفضاء السيبراني وخبراء تقنياته، ومن مختلف قطاعات الأنشطة السائدة في المجتمع الإيراني، ضمن مصفوفة معقدة، تضم عدداً هائلاً من المهام، وبتراتبية لا يمتلك المفتاح السحري لربط عناصرها المتوزعة، وتحويلها الى خطاطة امنية راسخة إلا صفوة من قيادات النظام التي تتوزع بين قمة الهرم الحكومي، ومؤسسة الحرس الثوري الإيراني، والباسيج، وبإشراف مباشر من قبل المرشد الأعلى للثورة الإسلامية.

من أجل هذا لن نجرؤ على الادعاء ان تحليلنا لهذه الهيكلة المعقدة سينجح بصورة تامة في وصف هوية ومهام هذه البنى المؤسسية، أو ان عملية تشخيص العلاقات القائمة بين هذه الكيانات، وأسلوب صناعة القرارات ووضعها حيز التنفيذ ستأتي متطابقاً مع تشعبات العلاقات الرابطة بين هذه العناصر المتكاثرة والمتداخلة بالوقت ذاته (*Wheeler,2013*).

ولأجل تبسيط وصف الهيكلة المؤسسية لأمن المعلومات في إيران، ومحاولة إزالة بعض من الغموض الذي يلفها، وتحديد هوية كياناتها، ذات الصبغة العسكرية، والأمنية، والتنظيمية، حاولنا تفكيك تركيبتها المعقدة الى مجموعة من الكيانات الثانوية، مع حرصنا على اعتماد مبدأ الهرمية المؤسسية الذي يميز الدور الذي يمارس من خلالها، بدءاً بقمة الهرم وانتهاء بالقاعدة العريضة التي ترسّخ ثوبت الكيانات وتماسكها.

بداية يمكننا تقسيم هذه الهيكلة المؤسسية بحسب الوظيفة التي تمارسها كل مركبة من مركباتها، والتي آثرنا الى تقسيمها الى الأقسام:

4. 1. الكيانات التي تعنى بالتخطيط الاستراتيجي:

تكاد تنفرد جهة واحدة بهذه المهمة الحيوية، هي المجلس الأعلى لالفضاء السيبراني، بعد أن كانت تتقاسمها أكثر من جهة، قبل عام 2012، والذي يعد حداً فاصلاً لبروز بنية مؤسسية متكاملة، خالية من سمة التشتت التي سادتها خلال أكثر من عقد من الزمان.

المجلس الأعلى للفضاء السيبراني[146] *High Council of Cyberspace*:

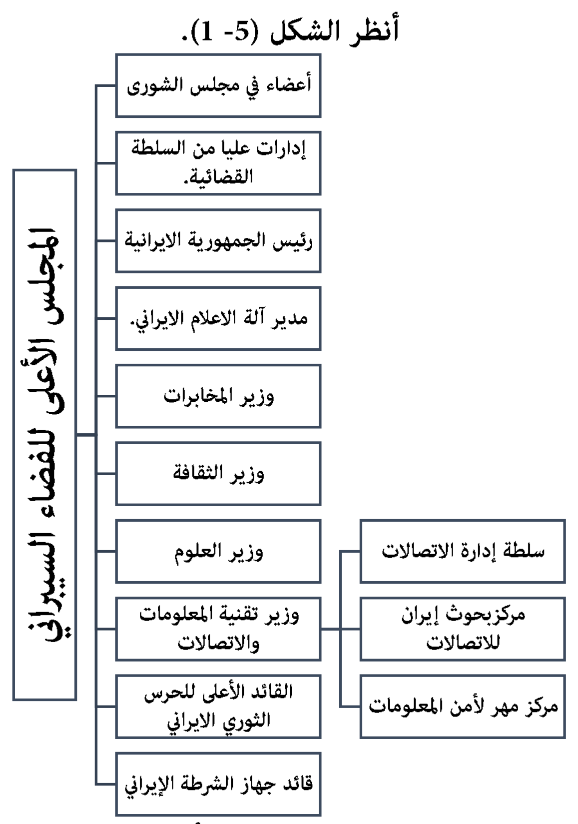
يستقر المجلس الأعلى لالفضاء السيبراني في قمة الهرم للهيكلة المؤسسية التي تخطط، وتعد الخطوط العامة لسياسات النظام الإيراني على صعيد ممارسة وتهيئة متطلبات عمليات الدفاع والردع السيبراني في إيران، والتنسيق فيما بين مختلف طبقات المؤسسات الحكومية لضمان انسيابية الأنشطة التي تتطلبها هذه المهمة مع توفير التخصيصات المالية واللوجستية لضمان نجاح هذه الخطط في تحقيق أهدافها وبلوغ غاياتها المرجوّة.

لم تكن ولادة هذا التشكيل المؤسسي بعيدة، فقد أنشئ المجلس في شهر مارس عام 2012 لتلبية أمر المرشد الأعلى للثورة علي خامنئي لإدارة كافة تفاصيل خطاطة إيران الوطنية في الفضاء السيبراني، وللتقليل من الترهل الوظيفي الناتج عن تكاثر الكيانات المؤسسية وتداخل صلاحياتها ومسؤولياتها، بحيث أصبح هذا المجلس مستقراً على قمة الهرم المؤسسي ـ السيبراني في البلاد.

وقد وفر للمجلس تشكيلة واسعة من الإدارات الحكومية العليا، تضمنت ممثلين عن: مجلس الشورى الإيراني، وإدارات السلطة القضائية العليا بالبلاد، وحضور لكل من: رئيس الجمهورية، ووزراء: كل من وزارة: المخابرات، وتقنية المعلومات والاتصالات، والثقافة، والعلوم، بالإضافة الى مدير آلة الاعلام الإيراني، والقائد الأعلى للحرس الثوري الإيراني، وقائد جهاز الشرطة الايراني (*Wheeler,2013*).

وقد التحق مع وزير تقنية المعلومات والاتصالات ممثلين عن: سلطة إدارة الاتصالات، ومركز بحوث اتصالات إيران، ومركز مهن لأمن المعلومات لكي تكتمل عناصر المجلس وتتكامل الصورة لديها عند وضع الخطط وصياغة الاستراتيجيات ـ

أنظر الشكل (5- 1).



الشكل (5 - 1) ـ الهيكلة المؤسسية للمجلس الأعلى للفضاء السيبراني في إيران.

[146] . سبق وأن ناقشنا هذا الكيان المؤسسي في فصل سابق، بتفصيل أكبر، لكننا سنحاول، في هذا المقام، مناقشة الدور الذي يمارسه ضمن تشكيلات الدفاع والردع السيبراني في إيران.

لذا فإن هذا المجلس بات يمثل أعلى مؤسسة حكومية، في إيران، تتحمل مسؤولية صياغة سياسات النظام على صعيد المحورين، الدفاعي، والهجومي في الفضاء السيبراني السيبراني، ومراجعة وإقرار الخطط التي تقترحها التشكيلات المؤسسية التي تقع تحت طبقته المؤسسية، بينما تمارس بقية الجهات المتوزعة في الطبقات الموالية مهام إعداد تفاصيل مفردات الخطط، والسعي الى تنفيذها وتوفير مستلزمات إنجاحها.

4. 2. الكيانات التنسيقية والداعمة:

حرصت الإدارة الحكومية، وبإشراف مباشر من المرشد الأعلى للثورة على توفير جميع أشكال الدعم المالي، واللوجستي، والتقني للتكتل الكبير الذي يعكف على حماية الكيانات السيبرانية والفضاء السيبراني الإيراني، ودرء الهجمات من خلال تنمية قدرات الردع السيبراني الوطني، وسخّرت له تخصيصات مالية تجاوزت 1 مليار دولار لتحقيق هذه الغاية وتطوير السلطان السيبراني الإيراني خلال مدة زمنية قصيرة بعد أن دقّ ناقوس تهديدات البرمجيات الخبيثة التي عاثت فساداً بمعدات برنامجها النووي الطموح.

وقد أولت اهتماماً كبيراً بمسألة توزيع حضور هذه التشكيلات على مساحة واسعة من الهرم الحكومي، حرصاً منها على منحه مرونة عالية في توفير الدعم، مع توفير عدة مستويات من أنماط الدعم التي تتوزع على قطاعات متعددة لضمان تكامل حلقتي الدعم والتنسيق وبما يتناسب مع الطموح غير المسبوق للنظام الإيراني في تحقيق قفزة نوعية على صعيد تنمية القدرات السيبرانية.

4 . 2. 1. مكتب التعاون والتنسيق التقني في مكتب الرئاسة:

توزعت جهود مكتب التنسيق والتعاون العلمي المشترك في مكتب رئيس جمهورية إيران بين المؤسسات الأكاديمية والبحثية التي تتوفر بكثافة في البلاد، من جهة، وبين الحدائق التقنية وحاضنات الابتكار لضمان توفير أرضية علمية وتقنية في البلاد تستثمر طاقات الكوادر الأكاديمية والبحثية في مجال أمن المعلومات والاتصالات[147] لاستنهاض عمليات إنتاج حصيلة معرفية وتقنية يمكن أن تستثمرها الشركات الصغيرة والمتوسطة التي استنبتت في حدائق التقنية أو رعايتها في حواضن الابتكار لإثراء البلاد بمنتجات وطنية تغني إيران عن التوجه نحو الحصول عليها من خارج البلاد، ولتوفير منتجات محلية تضمن عدم اختراقها، أو الكشف عن ثغراتها بواسطة الجهات التقنية التي ترتبط بالدول التي تناصب النظام الإيراني بالعداء.

ولترجمة استراتيجية إيران على صعيد بناء وتطوير قدراتها تحت مظلة مكتب التنسيق والتعاون العلمي في المكتب الرئاسي الايراني، وتنفيذ برامج استثمار الطاقات والقدرات الوطنية فقد وضعت نصب المكتب نصب عينيه المهام الآتية (*Siboni&Kronenfeld,2012*):

المهمة الأولى: تطوير تقنية المعلومات والاتصالات وتصنيع أدوات معلوماتية:

حرصت إيران على عدم الإفصاح عن تطور قدراتها في مجال تقنية المعلومات والاتصالات، بعيداً عن أنظار خصومها. فوجدت في مد جسور التعاون التقني مع المؤسسات الأكاديمية ومراكز البحوث مخرجاً مناسباً تستثمر فيه قدرات مواردها التقنية، مع ترسيخ أسس متينة لصناعة معلوماتية رصينة، تنأى بها عن الضغوط التي تتنشأ عن الحصار التقني المفروض على البلاد، بالإضافة الى ضمان كتمان ما نجحت الموارد التقنية الوطنية بتحقيقه في هذا المجال الحيوي.

---

[147] . بلغ عدد الأكاديميين والباحثين بمجال أمن الحواسب على صعيد ممارسة الهجمات والارتقاء بالكفاية الأمنية في إيران، عند أعتاب عام 2005 أكثر من 100 شخص توزع حضورهم على المؤسسات الأكاديمية والمعاهد البحثية بينما بلغ عدد الخبراء والتقنيين وقراصنة المعلومات الذين يعملون في المجالات التطبيقية لأمن المعلومات والكشف عن الثغرات السيبرانية، بصورة فردية، أو ضمن شركات توفر مشورة وخدمات أمنية، ومنتجات رقمية قد تجاوز بضعة آلاف (*Arquilla&Borer,2007*).

فقد لعب كل من مختبري الأبحاث والتطوير[148] في جامعة شريف للتقنية دوراً كبيراً في توفير أرضية متينة لإجراء برامج بحوث متخصصة لتوفير احتياجات البرنامج الإيراني على صعيد تقنية المعلومات والاتصالات في مجال الدفاع والردع السيبراني.

وفي خطوة لاحقة، أسس المجلس الأعلى لالفضاء السيبراني الإيراني، برنامجاً للدفاع السيبراني في جامعة الامام الحسين بطهران، وأنشأ مجموعة مراكز تقنية لإنتاج برمجيات مكافحة الديدان الخبيثة *Anti-Malware* التي تنتج في إيران، مع التوجه نحو تحليل المعمارية البرمجية للديدان الخبيثة التي تنتشر في الفضاء السيبراني للانترنيت، والتي أنشئت لاختراق الفضاء السيبراني الإيراني، ولإحداث تأثيرات ضارة على مختلف أشكال كياناته السيبرانية. كما شجعت هذه المراكز وبالتنسيق مع المؤسسات الأكاديمية على إعداد برامج تدريبية، ذات طابع أمني، لنشر الوعي الأمني لدى مستخدمي الانترنيت، والارتقاء بالمهارات والقدرات لدى كوادر المؤسسات الحكومية والقطاع الخاص على صعيد تمتين الحصانة الأمنية لشبكات المعلومات، ومكافحة الهجمات التي تمارس عليها بواسطة الفايروسات الحاسوبية والديدان الخبيثة (*Schwarz,2013*).

المهمة الثانية: التدريب وبناء القدرات السيبرانية:

أوكل جزء من مهمات تدريب الكوادر التي أوكلت لها مهما الدفاع عن الفضاء السيبراني، وممارسة الهجمات الى القطاع الأكاديمي الإيراني، المتمثل بالجامعات والمعاهد التقنية، وبعض مراكز الأبحاث المتخصصة بقطاع تقنية المعلومات والاتصالات[149].

وجاءت هذه الخطوة من الإدارة الحكومية لاستثمار ما يتوفر في البلاد من معاهد تقنية وجامعات تعنى بتخريج كوادر متخصصة في تقنية المعلومات والاتصالات، وهندسة الحواسب والنظم، وهندسة الاتصالات، ومراكز بحث وتطوير تلتحق بهذه المؤسسات الأكاديمية وما تتمتع به الكوادر الأكاديمية من معارف وخبرات تؤهلها لبناء قدرات وطنية متميزة دون اللجوء الى جهات خارجية في وقت قد فرض فيه حصار تقني صارم على البلاد (*Siboni&Kronenfeld,2012*).

وبينما أكد الباحثان (*Patterson&Smith,2005*) على الدور الكبير الذي مارسته جامعة شريف للتقنية في تخريج طيف واسع من الكوادر الأكاديمية والبحثية في قطاع أمن المعلومات وتطبيقاته، بيد انهما لم يعثرا في الفسحة الزمنية لدراستهما (عام 2004) على أدلة تثبت تورط هذه المؤسسة الجامعية في توظيف مهنة التدريس لتنشيط أنشطة القرصنة السيبرانية، أو إنتاج قراصنة معلومات لدعم أهداف النظام.

ويظهر أن البوابة السيبرانية التي خصصتها مجموعة *Ashiyane* لتدريب قراصنة المعلومات الإيرانيين ترتبط بوشائج متعددة مع الكثير من الجامعات الإيرانية المرموقة (مثل جامعة شريف للتقنية وجامعة أمير أكبر)، ممن لديها تحالفات استراتيجية مع مؤسسات الدفاع والردع السيبراني الإيرانية، بالإضافة الى توفير بوابة مفتوحة للتواصل مع روادها على مواقع شبكات التواصل الاجتماعي.

ولا تنفرد هذه المجموعة بامتلاك بوابة للتدريب، وإنما تشترك معها جلّ مجاميع القرصنة الموالية للنظام الإيراني، ودون وجود أي نمط من الحظر على أنشطتها وممارساتها التدريبية (*HP,2014*).

وقد أسهمت الخبرة الطويلة التي يتمتع بها أفراد مجموعة *Ashiyane* في مجال القرصنة السيبرانية، ورسوخ قدمها في شنّ هجمات موجعة على مواقع لخصوم النظام الإيراني، في حظوتها المميزة لدى مؤسسة الحرس الثوري الإيراني، والتي كلفتها بصورة رسمية للنهوض بمهمة تدريب فصائل جيش إيران السيبراني *ICA* (*HP,2014*).

---

148 . مركز البحوث المتقدمة لتقنيات المعلومات والاتصالات، ومركز بحوث الاتصالات المتقدمة.

149 . تبوأت مكانة الصدارة في هذا المجال جامعة شريف للتقنية، وجامعة أمير أكبر للتقنية حيث استوطنت هاتين الجامعتين في العاصمة طهران.

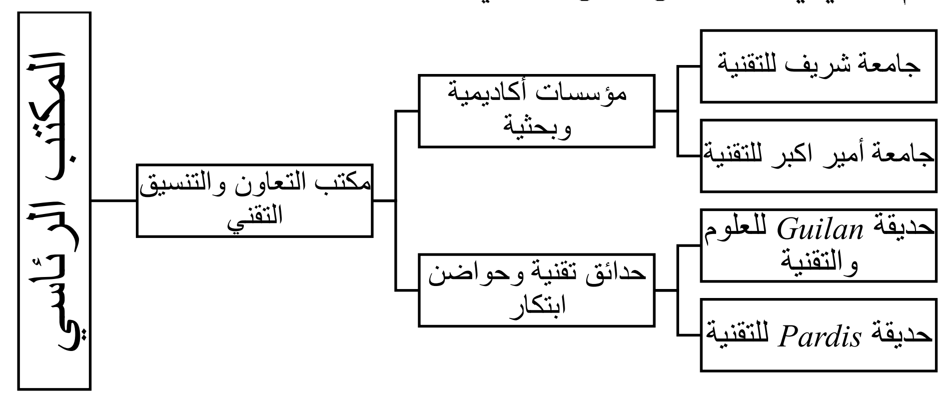
وبالإضافة الى برامج التدريب المهني ـ المرخصة للقراصنة *Certification Programs*، وتوفير منح للدراسات العليا في جامعات إيرانية مرموقة، اعتمد النظام الإيراني نهج نشر ألعاب القرصنة لجذب وتجنيد قراصنة المعلومات وتدريب قراصنة المعلومات والارتقاء بمهاراتهم وتعميق خبراتهم بهذا المجال. وقد انتشرت كثير من برامج محاكاة القرصنة ولعب الحرب *War Games* والتي ساعدت الإدارات الأمنية على تحديد مستوى المهارة الذي يمتلكه القرصان الإيراني من خلال هوية الأهداف التي نجح باختراقها، وحجم التأثير الذي نجح بتحقيقه في مواقع الخصم.

ويضاف الى هذه البيانات مجموعة الوثائق والشواهد التي يوفرها قراصنة المعلومات الإيرانيين في مواقع تتبع أنشطة القرصنة العولمية مثل موقعي *Zone-h.com & Zone-hc.com* والتي تعين مؤسسة الحرس الثورية الإيراني، ومنظمة الباسيج على تشخيص القراصنة المتميزين والمباشرة بالسعي نحو جذبهم وتجنيدهم مع الفصائل السيبرانية التي تعمل بمعية الجيش السيبراني الإيراني، أو الباسيج (*HP,2014*).

المهمة الثالثة: بناء قدرات الطلبة الإيرانيين في مجال أمن المعلومات والاتصالات:

توسيع قاعدة المعرفة العلمية والممارسات المهنية في قطاع تقنية أمن المعلومات، والكشف عن الثغرات الأمنية، وشد اهتمام الملتحقين في الجامعات الإيرانية نحو ممارسات القرصنة السيبرانية، بشقيها الأبيض والأسود، من خلال إدراج مناهج علمية وتقنية في مجال أمن المعلومات، واختراق نظم الشبكات، والتشفير السيبراني في البرامج الدراسية لكيات علوم الحاسب، وهندسة الحواسب والنظم، وتوجيه اهتمام الطلبة الى هذه الحقول مع تطوير برامج الدراسات العليا بهذه الحقول لإ نتاج جيل من الخريجين الذين ستوفر لهم الإدارة الحكومية فرصاً للعمل في مؤسساتها، بالإضافة الى الحاقهم بشبكة من الأنشطة التي تتوزع بين نشاطات بحثية لتطوير النظم البرمجية وسد الفجوات الأمنية، أو إنتاج أدوات وبرمجيات خبيثة لدرء المخاطر وردع خصوم البلاد عن التقرب من فضائها السيبراني، وتجنيد آخرين للعمل ضمن فصائل جحافلها السيبرانية التي تعمل ضمن المؤسسات الأمنية أو العسكرية، مع تكوين قاعدة وطنية من المهارات الوطنية في هذا الحقل الحيوي[150].

وسنحاول المرور سريعاً للكشف عن أهم المؤسسات الأكاديمية والبحثية، والحدائق التقنية وحاضنات الابتكار التي تعمل بمعية مكتب التنسيق والتعاون المشترك في مكتب رئيس الجمهورية مع بيان بعض الأنشطة التي تمارسها ضمن خطط النظام الإيراني في مجال الدفاع والردع السيبراني ـ أنظر الشكل (5- 2).



الشكل (5- 2) ـ التشكيلات المرتبطة بمكتب التعاون والتنسيق التقني في مكتب رئيس الجمهورية الإيرانية.

[150] . منذ عام 2007 تبنت الإدارة الحكومية في إيران برامج وحوافز تشجيعية للمتميزين من الطلبة الإيرانيين منها استثناءهم من الخدمة العسكرية في حالة عملهم في مشاريع وطنية ذات طابع استراتيجي مثل المشروع النووي الإيراني أو يخدم سياسة الدفاع والردع السيبراني في البلاد، بالإضافة الى الدعم المالي والمعنوي.

4 .2 .2. المؤسسات الأكاديمية والبحثية:

تمتلك إيران عدداً كبيراً من المؤسسات الأكاديمية (جامعات ومعاهد ومراكز بحوث) عريقة وتتبوأ مكانة متقدمة في رصانتها على صعيد المنطقة، وترقى بعضها الى مستوى مرموق على المستوى العولمي.

وينتمي الى هذه المؤسسات الرصينة حجم كبير من الموارد البشرية التي تمتلك خبرات عميقة، تمنحها القدرة على المساهمة في البرنامج الإيراني الخاص بتطوير تقنيات، وأدوات المعلومات والاتصالات، وبناء قدرات الموارد البشرية الوطنية والذي سيثمر عن توفير حجم كبير من التخصيصات المالية في وقت ازداد فيه ضغط كمّاشة الحصار المفروض على إيران.

وقد أدرجت الإدارة الحكومية هذه التشكيلات المؤسسية ضمن البناء المؤسسي الشامل لدعم قدراتها الدفاعية وقوة الردع السيبرانية في الفضاء السيبراني، فانتخبت مجموعة من الجامعات، والمعاهد التقنية، ومراكز البحوث للمساهمة في مهام محددة تدعم استراتيجيتها الوطنية لتطوير حضورها الأمني والعسكري في الفضاء السيبراني.

حرص النظام الإيراني على إنشاء بنية تحتية متماسكة، لدعم أنشطة البحث والتطوير في قطاع تقنية المعلومات، مع توفير بيئة حاضنة لتسيير برامج تدريبية رصينة في أكثر من مؤسسة أكاديمية بالبلاد. وتبدو جلية للعيان أوجه التنسيق والتعاون المشترك بين البرنامج الحكومي للدفاع وقوة الردع السيبراني وبين المؤسسات الأكاديمية في كل من: جامعة شريف للتقنية، جامعة الشهيد بهشتي، وجامعة مالك الأشتر التي تعمل ضمن حلقة مؤسسة الحرس الثوري الإيراني.

وقد أوكل لكل جامعة، أو معهد تقني، أو مركز بحث علمي مهمة محددة، تشكّل جزءاً محدداً من أجزاء فسيفساء المشروع الإيراني الذي تروم الإدارة الحكومية تنفيذه لضمان بناء قدراتها الدفاعية، وتعزيز سلطانها السيبراني في فضاء الفيض السيبراني، وبنهج يحاكي الى حد كبير، النهج الذي اعتمده في بناء قدرات مشروعها النووي الذي استعصى على الكثير من خصومها تفكيك بنيته الراسخة الى عناصرها الولية في سبيل الكشف عن اللبنات التي ارتكز اليها هذا المشروع الي لا يكاد يتوافق مع القدرات الظاهرة لدولة نامية مثل إيران، وفي ظل حصار تقني خانق قد فرض على الكثير من أنشطتها ونزعات تواصلها مع المجتمع التقني العولمي.

فسخّرت جميع القدرات المتوفرة في مؤسساتها الأكاديمية، والبحثية، واستثمرت الخبرات والمهارات التي تمتلكها مواردها البشرية لدعم نجاح استراتيجيتها السيبرانية، واستطاعت أن تحقق قفزات ملموسة (خلال بضع سنوات) في مضمار الحروب السيبرانية، أدهشت خصومها واوقعتهم في حيرة شديدة عند محاولة تفسير هذه الطفرة السيبرانية الكبيرة[151].

وقد عقدت إدارات المؤسسات الجامعية (التي انتخبت من بين أفضل الجامعات في إيران بحسب رصانتها العلمية، تتوفر فيها كوادر عملية وتقنية متميزة، وينتظم بأقسامها الهندسية والحاسوبية خيرة الطلبة الإيرانيين) شراكات وطيدة مع مؤسسات متعددة تنتمي الى الهيكلة المؤسسية للدفاع والردع السيبراني، وبمساهمة فاعلة من مراكز البحوث التقنية المنتشرة في البلاد، وبمباركة من قبل المجلس الأعلى لالفضاء السيبراني في إيران، للمباشرة ببرنامج عمل مشترك متعدد الأهداف، توفر له الحكومة الدعم المالي واللوجستي المطلوب، بينما يشرف المجلس الأعلى على رعاية البرنامج وتنسيق المهام بين الجهات التي تعمل تحت مظلته. ويمكن إيجاز المهام التي التزم بها الشركاء

[151] . إن مراجعة سجلات أنشطة الجامعات الإيرانية، تظهر أن تدريس أسس البحث وممارساته في قطاع إدارة شبكات الحواسب، وأمن المعلومات والتشفير، لم تقتصر على جامعتي شريف وأمير كبير للتقنية فحسب، فهناك بصمات واضحة لجامعات أخرى مثل جامعة أصفهان، وجامعة أصفهان للتقنية اللتان تديران برامج مشابهة، وضمن طيف واسع من الاختصاصات الأكاديمية الصرفة والتطبيقية، لضمان ترسيخ قاعدة عريضة أمن المعلومات وحصانة النسيج الشبكاتي في البلاد (*Arquilla&Borer,2007*).

ولعل أهم هذه الكيانات التي عملت ضمن دائرة مشروع بناء القدرات الوطنية الدفاعية وقوة الردع السيبراني، وسخرت الكثير من قدراتها المادية والبشرية للمساهمة بهذا المشروع:

4 . 2 . 2 . 1 . جامعة شريف للتقنية *Sharif University of Technology*:

احتلت جامعة شريف للتقنية (بحسب تصنيف موقع *Rank* الشهير[152]) المرتبة 401 من أفضل 500 جامعة بالعالم ومن أفضل 70 جامعة تقنية، ومن أفضل 60 جامعة هندسية بالمنطقة في عام 2016. وقد بلغ عدد طلبتها 10,977 طالباً في الدراسات الأولية والعليا، بينما بلغ عدد كوادرها التدريسية والبحثية 588 أستاذاً، بينما بلغت نسبة عدد الطلبة لكوادرها التدريسية 18.7 طالب/كادر تدريسي.

وقد نجحت في إنتاج عدد كبير من الحاصلين على الشهادات العليا الذين أغنوا البلاد بحصيلة علمية رصينة. فبلغ عدد الحاصلين على شهادة الدكتوراه من هذه الجامعة 1,049 طالباً، بينما بلغ عدد الحاصلين على شهادة الماجستير 1,381 طالباً.

ولم يقتصر تفوقها على الجانب الأكاديمي الصرف، فاحتلت على صعيد ممارسة البحث العلمي (ضمن احصائيات عام 2016) المرتبة 68 بين جامعات المنطقة، والمرتبة 224 بين جامعات العالم المختلفة[153].

وتعد هذه الجامعة من المؤسسات الأكاديمية والبحثية الرائدة على صعيد تخصصات أمن شبكات المعلومات، وأمن نظم المعلومات ونسيجها الشبكاتي، وتشفير المعلومات، وتقنيات القرصنة السيبرانية بالإضافة الى التنقيب عن مواطن الثغرات الأمنية في نظم المعلومات والتطبيقات البرمجية[154].

وتميزت هذه الجامعة العريقة بتوجهها نحو إنشاء ورعاية عدة مراكز ومعاهد تعنى بالبحوث العلمية والتطبيقية ناهز عددها على 16 مركزاً ومعهداً. لعل اكثرها أهمية على صعيد مسائل المنعة والردع السيبراني، مركز البحوث المتقدمة في مجال تقنية المعلومات والاتصالات *Advanced Information and Communication Technology Research Center (AICTC)*، ومعهد البحوث المتقدمة في الاتصالات *Advanced Communications Research Institute* ومركز بحوث الالكترونيات *Electronic Research Center*، ومركز شريف لبحوث الفيزياء التطبيقية *Sharif Applied Physics Research Center*. وقد سخّرت هذه المراكز والمعاهد البحثية قدراتها البحثية والتقنية لدعم الاحتياجات التقنية لأمن المعلومات والاتصالات، وتوفير أدوات معلومات وتطبيقات برمجية تدعم أنشطتها الدفاعية والهجومية من خلال انشاء شركة صغيرة أو متوسطة تدعمها الحكومة بتمويل مالي لبدء عملها، وترسيخ حضور منتجاتها المحلية[155] (*Patterson&Smith,2005*).

---

152 . راجع صفحة الموقع:
https://www.timeshighereducation.com/world-university-rankings/sharif-university-of-technology

153 . وفق البيانات التي نشرها الموقع:
http://www.usnews.com/education/best-global-universities/sharif-university-of-technology-502898

154 . يعد البروفيسور شاهرام بختياري أحد الرواد بهذا المضمار في هذه الجامعة منذ أكثر من عقد الزمان (*Arquilla&Borer,2007*).

155 . آتت جهود كوادر الجامعة وطلبتها ثمارها عندما نجحت الجامعة في المسابقة العالمية التي عقدت في شنغهاي عام 2006 بالحصول على المرتبة 13 عولمياً على صعيد تقييم أنشطة نخبة من طلبتها بتخصصات عمليات شبكات الحواسب *CNO*، فتقدمت على الكثير من الجامعات الأمريكية، باستثناء معهد *Massachusetts Institute of Technology* الشهير والذي احتل المرتبة الثامنة (*Arquilla&Borer,2007*)، الأمر الذي يؤكّد على قدرة هذه المؤسسة الأكاديمية على إنتاج مواهب في ميدان أمن المعلومات والتطبيقات البرمجية الداعمة لهذا الحقل، وممارسة تقنيات الكشف عن الثغرات السيبرانية، والقرصنة السيبرانية.

4 . 2 . 2 . 2 . جامعة أمير كبير للتقنية *Amirkabir University of Technology*:

احتلت جامعة أمير كبير للتقنية (بحسب تصنيف موقع *Rank* الشهير[156]) المرتبة 501 من أفضل 600 جامعة بالعالم ومن أفضل 70 جامعة تقنية، ومن أفضل 79جامعة متخصصة بعلوم الحاسب والهندسة[157] بالمنطقة في عام 2016. لقد تميزت هذه الجامعة بمجموعة من الحقول العلمية والهندسية مما منحتها فرصة احتلال مواقع متقدمة على صعيد تراتبية جامعات العالم. فعلى صعيد أنشطتها العلمية والأكاديمية بحقول العلوم الهندسية احتلت المرتبة 151-200 خلال العامين 2014-2015، بينما احتلت المرتبة 101-150 في علوم الحاسب خلال العامين 2013،2015، بينما احتلت المرتبة 151-200 خلال العامين 2012، 2014 واحتلت المرتبة 151-200 في حقل علوم الرياضيات خلال العام 2015[158].

إضافة الى هذه الإنجازات الأكاديمية يستضيف قسم هندسة الحاسب وتقنية المعلومات فيها مخابر بحوث أمن المعلومات *Data Security Research Laboratory*، حيث تتوفر فيه جميع أشكال الدعم العلمي والتقني لأنشطة البحث والابتكار في تخصصات أمن الحاسب، والمعلومات، والاتصالات. كما يوفر هذا المركز برامج تدريبية رصينة لدعم الكوادر الهندسية وللمشتغلين بعلوم الحاسب وتطبيقاته للارتقاء بمهاراتهم، وقدراتهم التقنية (*Arquilla&Borer,2007*).

وقد عززت الدراسة التي قامت بها كوادر تحريات الأمن السيبراني في شركة *Hewlett Packard* الأمريكية عام 2014 الشكوك حول وجود تنسيق مباشر مع كبريات الجامعات الإيرانية (مثل جامعة شريف للتقنية، وجامعة امير أكبر للتقنية، وجامعة الشهيد بهشتي) والمتحالفة مع النظام الإيراني مع مجاميع القرصنة السيبرانية مثل: مجموعة *Ashiyane*، ومجموعة *Shabgard* على صعيد إدارة بوابة تدريب قراصنة المعلومات وتوفير مناهج التدريب. كذلك وجدت أن هذه البرامج قد بدأت تتلقى الدعم من منظمة الطاقة الذرية الإيرانية، بعد أن تعرضت منشآتها لهجمات الفايروس الخبيث *Stuxnet* في خطوة لتوفير مستوى مقبول من الحماية الأمنية لمنشآتها إزاء تصعيد الهجمات السيبرانية الأمريكية ـ الإسرائيلية ضد المشروع الإيراني خلال السنوات الأخيرة (*HP,2014*).

4 . 2. 3. حدائق التقنية وحواضن الابتكار:

يشرف مكتب التعاون والتنسيق التقني في مكتب رئيس جمهورية إيران على سلسلة من المهام الداعمة لبرنامج إيران للدفاع والردع السيبراني. وتعمل بمعيته مجموعة من حدائق الابتكار والحواضن التقنية التي تسخّر قدراتها لهذا البرنامج الطموح.

وقد أوكلت للحدائق التقنية وحواضن الابتكار مهمة ترسيخ قاعدة تقنية عريضة قادرة على احتضان ورعاية عدد كبير من المشاريع صناعية صغيرة، وأخرى متوسطة لإنتاج الأدوات والتطبيقات البرمجية التي تفتقر اليها البنية التحتية للمعلومات والاتصالات في ترسيخ أمنها، وسد فجواتها السيبرانية ولكل من عتاد الحواسب والشبكات، والتطبيقات البرمجية التي تكافح آثار البرمجيات الخبيثة بجميع أشكالها.

---

[156] . راجع صفحة الموقع:
https://www.timeshighereducation.com/world-university-rankings/amirkabir-university-technology?ranking-dataset=133819

[157] . بلغ عدد طلبتها 14,080 طالباً، في الدراسات الأولية والعليا.

[158] . راجع صفحة الموقع:
http://www.shanghairanking.com/World-University-Rankings/Amirkabir-University-of-Technology.html

وتعد كل من حديقة *Guilan* للعلوم والتقنية[159]، وحديقة *Pardis* للتقنية[160] من الجهات الفاعلة التي تعمل تحت مظلة مكتب التعاون والتنسيق المشترك لتوفير مختلف أشكال الدعم التقني لبرنامج النظام الإيراني السيبراني بعد أن خطط لهذه الحديقة التقنية أن تناظر في أنشطتها التقنية والتصنيعية الدور الذي يمارسه وادي السيلكون بالولايات المتحدة في دعم ورعاية صناعة متقدمة في مجال تقنية المعلومات والاتصالات، حتى أطلق عليها البعض وادي السليكون الإيراني *Iranian Silicon Valley* (*Arquilla&Borer,2007*).

ويبدو أن هناك تنسيقاً وتعاوناً علمياً وتقنياً وثيقاً بين مراكز البحث والتطوير في جامعة شريف للتقنية، من جهة، والشركات الوليدة في حديقة *Pardis* التقنية من جهة أخرى وذلك عن طريق اقتناء براءات الاختراع التي ولدت في مخابر جامعة شريف التقنية وتحويلها الى منتجات معلوماتية بواسطة الشركات المقيمة في الحديقة التقنية. فشركة شريف للأدوات والتطبيقات البرمجية الأمنية *Sharif Secure Ware*، والتي ولدت في ربوع جامعة شريف للتقنية، تعد من الشركات الخمس والأربعين التي توطنت في البيئة الحاضنة لهذه الحديقة التقنية، وباتت تتلقى دعماً مباشراً لتطوير أنشطتها منذ عام 2004 (*Arquilla&Borer,2007*).

وقد توفرت معلومات لدى الباحثين (*Patterson&Smith,2005*) تؤشر الى أن كوادر البحث العلمي والتطوير التقني في مختبرات جامعات أمير أكبر فقد بدأت بممارسة دور مهم في تطوير تقنيات التشفير، والتنقير عن الفجوات السيبرانية المحتملة في التطبيقات البرمجية، واقتراح حلول لتجاوز سعي الغير الى استغلال هذه الثغرات الأمنية لممارسة تهديدات معلوماتية على النسيج الشبكاتي الوطني.

4 . 2 . 4 . مركز إيران لبحوث الاتصالات *ITRC*:

في البداية، سعت الإدارة الحكومية في إيران الى دعم أنشطة البحث والتطوير في مجالات أمن المعلومات والاتصالات لتلبية احتياجاتها في إحكام الحصانة الأمنية لجميع أشكال الاتصالات التي تسري في الفضاء الاتصالي الإيراني. وكانت ولادة مركز إيران لبحوث الاتصالات[161]، بأقسامه التقنية الأربعة استجابة لهذا السعي، من خلال توفير بيئة تقنية وطنية تسخر القدرات العلمية والتقنية لطرح حلول تتعلق بالكفاية الأمنية لشبكات المعلومات والاتصالات في عموم البلاد.

اقتصرت أنشطة المركز خلال العقود الثلاثة الأولى من انشائه على توفير حلول لوزارة تقنية المعلومات والاتصالات. بيد أن الحصار التقني الذي فرض على إيران منذ تولي نجاد لرئاسة إيران، وتفاقم التهديدات والهجمات السيبرانية على البنية التحتية للمعلومات والاتصالات في إيران، قد أجبر النظام الإيراني على تسخير القدرات العلمية والتقنية في هذا المركز لتوجيه عنايتها وتخسير قدراتها لدعم برنامج تنمية القدرات الدفاعية وقوة الردع السيبراني الإيراني، لتجاوز عقبة الحصار التقني من جهة، وتوفير حلول وطنية باتت تمس الأمن الوطني للبلاد في مجال الفضاء السيبراني (*Arquilla&Borer,2007*).

---

[159] . تربط مكتب التنسيق التعاون المشترك علاقة حميمة مع حديقة *Guilan* للعلوم والتقنية منذ بضعة عقود فقد أنشئ المكتب في عام 1984 لتوفير دعم لمكتب رئيس الجمهورية الإيرانية وتذليل العقبات أمام خططه لتطوير وتوطين التقنيات الحديثة بالبلاد، بينما أنشئ المركز في عام 1989 بوصفها لبنة أساسية لممارسة أنشطة البحث والتطوير وتوطين التقنيات في البلاد، ثم تحولت الى حديقة تقنية في عام 2002 تضع نصب عينيها تطوير تقنيات المعلومات والاتصالات وتطبيقاتها في البلاد.

[160] . أنشئت حديقة *Pardis* التقنية عام 2001 وجعل مستقرها في ضواحي مدينة طهران، وخطط لها لأن تكون بيئة حاضنة للبحوث ورعاية نمو شركات وطنية تعنى بالتقنيات الحديثة، والتي تعد تقنيات أمن المعلومات والاتصالات، وتطبيقاتها البرمجية جزءاً من اهتماماتها المتشعبة.

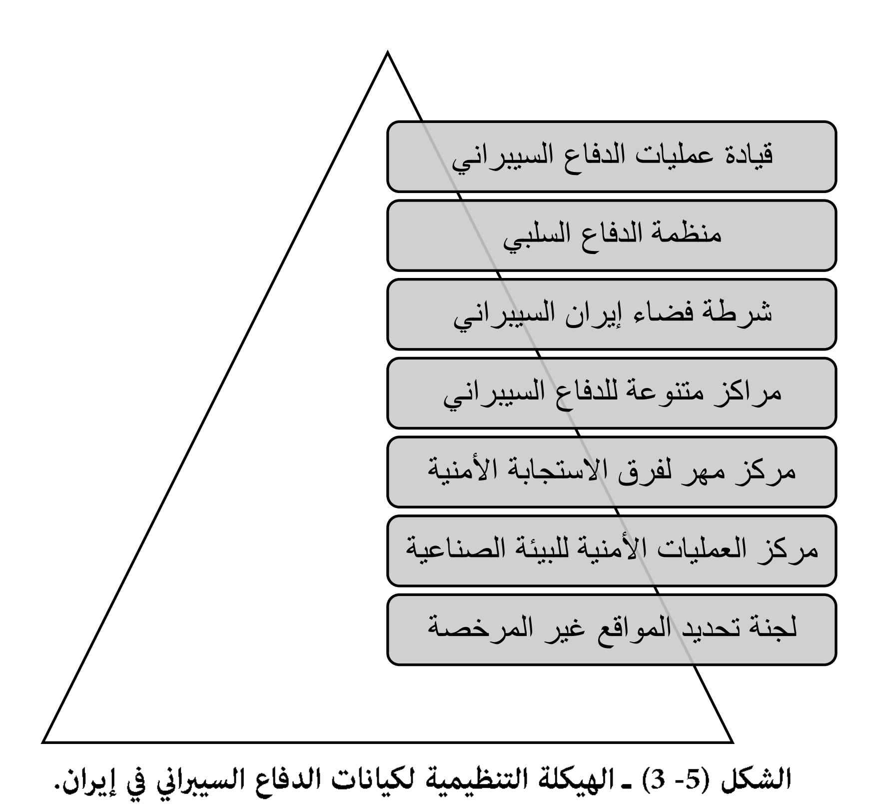
[161] . يعد مركز إيران لبحوث الاتصالات (*ITRC*) من المراكز البحثية والتقنية العريقة، والذي تمتد جذوره الى عقد السبعينات من القرن الماضي، عندما أنشئ في عام 1970 لمباشرة أنشطة البحث والتطوير تحت مظلة وزارة تقنية المعلومات والاتصالات.

4 . 3 . كيانات الدفاع السيبراني:

تزايد اهتمام القيادات الإيرانية بطبيعة الدور الجوهري الذي يمكن أن تمارسه الهجمات والحروب السيبرانية، وتأثيراتها العميقة على البنى التحتية للمعلومات والاتصالات، لخصوم الثورة الإسلامية بواسطة أوات تقنية المعلومات والاتصالات المتوفرة بسخاء على شبكة الانترنيت، إضافة الى النهج الناعم الذي تمارسه في أعماق فضاء الفيض السيبراني، حيث غياب الهوية، واضمحلال الحدود الجغرافية، مما يمنح الجهة التي تمارسها مرونة أكبر في ممارسة نشاطها بعيداً عن أعين المراقبين.

لم تكن الإدارة الإيرانية الوحيدة في هذا التوجه والاهتمام بتشكيل كيان أمني وعسكري لإدارة دفة ملف أمن فضاء الفيض السيبراني والتعامل بحزم مع التهديدات الأمنية، وصد الهجمات السيبرانية المحتملة التي يمارسها الخصوم على حمى الفضاء السيبراني الوطني، فقد هرعت دول كثيرة الى تشكيل هذه الكيانات وسعت الى دعمها وترسيخ جذورها ضمن هيكلة مؤسساتها العسكرية والأمنية.

وسنحاول خلال هذه الفقرة بذل ما في وسعنا في تحليل عناصر البنية المؤسسية لمأسسة عمليات الدفاع والردع السيبراني الإيراني، مع تتبع تراتبية هذه البنية، والكشف عن أهم الارتباطات القائمة بين كياناتها لكشف جزء ولو يسير من الفسيفساء المعقدة التي تعمد النظام الإيراني على تشكيلها لتعمية الأنظار عن طبيعة وحجم السلطان السيبراني الذي يتمتع به النظام، مع السعي الى تغييب الجهات الفاعلة ومحاولة توطينها خارج نطاق سلطة الحكومة لدفع أصابع الاتهام التي تكاثرت بعد بروز مطالع برنامجها النووي، وبرامج الصواريخ البالستية، وغيرها من البرامج التي باتت تؤرق بلدان المنطقة وبلدان العالم الغربي ـ أنظر الشكل (5- 3).



الشكل (5- 3) ـ الهيكلة التنظيمية لكيانات الدفاع السيبراني في إيران.

4 . 3 . 1 . قيادة عمليات الدفاع السيبراني:

أنشئت قيادة الدفاع لالفضاء السيبراني (*Gharagah-e Defa-e Saiberi*) في شهر نوفمبر من عام 2010، في إيران، والحقت ضمن تشكيلات منظمة الدفاع المدني[162]، والتي تعد بدورها، إحدى تشكيلات القوات المشتركة للقوات المسلحة الإيرانية. وقد بَرّر البعض تشكيل هذه القوة بوصفها رد فعل، واجراء فوري بعيد الهجمات الشرسة التي استهدفت مشروع تخصيب اليورانيوم الإيراني، وإحداث اضرار بالغة في أجهزة الطرد المركزي بواسطة الفايروس الخبيث *Stuxnet* في بداية العام ذاته (*HITCON,2013*).

ويستضاف ضمن الهيكل التنظيمي لهذا التشكيل مجموعة واسعة من ممثلي الوزارات الحكومية، مثل: وزارة تقنية المعلومات والاتصالات، ووزارة الدفاع، ووزارة المخابرات، ووزارة الصناعة لضمان تكامل خططه وممارساته لدرء المخاطر والتهديدات على قطاعات الدولة المختلفة (*Wheeler,2013*).

وقد أوكلت للتشكيل الجديد مهمة توفير بيئة رقمية آمنة في عموم الفضاء السيبراني بالبلاد، ودرء مخاطر التهديدات المحتملة على الفضاء وبنيته التحتية للمعلومات والاتصالات. ونتيجة لتعاظم المخاطر السيبرانية واقتناع الإدارات التشريعية والحكومية بالبلاد بأهمية التحرك السريع لتطوير قدرات ومهارات كوادر وإدارة هذا التشكيل، فقد هرعت المنظمة، وبدعم مباشر من القيادة العامة للقوات المسلحة الى توسيع نطاق مهامه، وتجنيد عدد كبير ممن خبروا التعامل مع التهديدات الأمنية، وآخرين ممن اتقنوا صنعة القرصنة السيبرانية للالتحاق بصفوف هذا التشكيل لضمان تماسكه وقدرته على النهوض بالمهام الأمنية الجسيمة التي أوكلت إليه في وقت أصبحت الكثير من الكيانات السيبرانية، والمؤسسات المهمة عرضة لهجمات متكاثرة من الولايات المتحدة وحليفتها إسرائيل بقصد تضييق الخناق على النظام الإيراني، وإحداث شلل جزئي أو كلي في برنامج إيران النووي.

4 . 3 . 2 . منظمة الدفاع المدني *Passive Defense Organization*:

أبصرت منظمة الدفاع المدني (*Sazeman-e Padafand-e Gheyr-e Amel*)[163] النور خلال ولاية الرئيس السابق أحمدي نجاد، وبتوجيه مباشر من المرشد الأعلى علي خامنئي، وتركت مهمة تعيين قائدها الى القائد الأعلى للقوات المسلحة الإيرانية، الجنرال حسن فيروز آبادي. في البداية، أوكلت لمنظمة الدفاع المدني، مهمة توفير كافة مستلزمات حماية مشروع إيران النووي، من خلال اعتماد معايير امنية مشددة لضمان حصانته قبالة التهديدات والهجمات المحتملة للمناهضين الأساسيين: الولايات المتحدة وإسرائيل، ولتغييب بعض تفاصيل حضور منشآته أمام لجان التفتيش الدولية التي قد تندبها منظمة الطاقة الذرية لمراقبة النشاط الذي يمارس في هذا القطاع (*Porter,2010*).

ومع بدايات عام 2012 أوكلت لها (بحسب تصريح قائدها الأعلى غلام ميرزا أميري) مهمة التقليل من حجم المخاطر المحتملة عن التهديدات السيبرانية، وعمليات التوّغل في الفضاء السيبراني الإيراني باستخدام أدوات الحروب الناعمة بعيداً عن استخدام القوة العسكرية. وقد أمر القائد الأعلى قيادة هذه المنظمة بإنشاء قاعدة دفاع رقمية في إيران،

---

162 . في عام 2011، أعلن غلام رضا جليلي، رئيس منظمة الدفاع السلبي *Passive Resistance Organization*، عن مباشرة مركز عمليات حرب المعلومات بالجمهورية الإسلامية *Cyber War Headquarters of The Islamic Republic of Iran* عمله وأنه سيقوم بمواجهة أعداء إيران المنتشرين في الفضاء السيبراني، وأن المركز سيمارس مهامه بالدفاع عن الحياض السيبرانية لإيران بإشراف مباشر من مؤسسة المقاومة السلبية (*MAI,2011*).

163 . يستخدم اصطلاح الدفاع السلبي، في قاموس الاصطلاحات العسكرية للجيش الأمريكي، لوصف مجموعة من الأنشطة التي تمارسها مؤسسات محددة لتقليل آثار التدمير التي قد تحصل نتيجة لممارسات عدائية على مؤسسات البلاد دون وجود نية لمباشرة فعل مضاد (*http://www.militaryfactory.com/dictionary/military-terms-defined.asp*).

تناط بها مهمة الكشف عن التهديدات السيبرانية التي تمارس ضد إيران، وتتبع الممارسات المشبوهة التي تريد النيل من البنية التحتية للمعلومات وأمن المعلومات الوطني (*ONI,2013*).

حيث أشار غلام رضا جليلي، رئيس هذه المنظمة، أثناء لفعاليات مؤتمر الأمن الوطني لالفضاء السيبراني (والذي عقد خلال يومي 18 و19 فبراير عام 2012) وحضرته مجموعة مجموعة من الشخصيات المهمة، الى أن إيران باتت تعد الضحية الأولى لحروب المعلومات، في إشارة الى الهجمات التي مورست بواسطة الفايروس الخبيث *Stuxnet* على أجهزة الطرد المركزي لتخصيب اليورانيوم.

وفي مقام آخر، لخّص غلام رضا جليلي، توجهات النظم الإيراني صوب التحضير لخطة الطوارئ التي ستعتمد لإدارة مجال السجال السيبراني الذي قد يندلع في الفضاء المدني، وأعلن أن ذلك سيتم من خلال إنشاء المزيد من مؤسسات فضاء الفيض السيبراني، وضمن قطاعات متعددة من تشكيلات الإدارة الحكومية، وتوجيه الاهتمام نحو قطاع الدفاع عن الكيانات السيبرانية، والكشف عن الفجوات المقيمة في النسيج الشبكاتي بالبلاد، مع تدريب المزيد من الكوادر الأكاديمية المنتخبة ممن يمتلكون مهارات وقدرات متميزة على صعيد القرصنة السيبرانية، ومراجعة بناء القدرات من خلال إجراء المناورات للوقوف على مستوى تكامل الأداء بين جميع القطاعات المساهمة لضمان احتواء ودرء الأخطار المحتملة عن الهجمات التي ستستهدف البنى التحتية للمعلومات والاتصالات[164]. وبحسب تصريحاته في 2013 فقد بلغ عدد المناورات التي أجرتها منظمة الدفاع المدني، خلال السنتين 2011 و2012 أكثر من 500 مناورة في عموم البلاد لتأكيد حضور مستوى مقبول من الحصانة الأمنية ـ السيبرانية تجاه التهديدات المحتملة (*Mansharof,2013*).

وقد تسارعت أنشطة منظمة الدفاع المدني في قطاع الفضاء السيبراني، فأعلنت في عام 2013 عن التحضير لعدة مناورات رقمية ـ ميدانية تشارك فيها جميع المؤسسات الإيرانية للتأكد من مستوى الحصانة الأمنية المتوفرة لدى كل منها واختبار قدرات مواردها البشرية على صد الهجمات السيبرانية المحتملة، واحتواء آثارها بما يضمن الأمن السيبراني الوطني. كذلك فإن كوادرها استمرت بالعمل على إعداد لوائح تنظيمية ومعايير للبنى التحتية الأساسية في إيران لضمان حصانتها غزاء التهديدات والهجمات السيبرانية المتكاثرة والخطيرة[165].

في البداية، أنشئت منظمة الدفاع المدني عام 2003 أنيطت بها مهمة الدفاع المدني المدني، دون أن يكون لها صلة بأنشطة ذات صبغة عسكرية. بيد أن اللجنة الدائمة لهذه المنظمة قد ضمت إليه ممثلين من القوات المسلحة، ومن مؤسسات حكومية متنوعة لدعم نشاطه وضمان التنسيق المشترك مع الجهات المستفيدة من أنشطته. وقد باشرت سكرتارية اللجنة عملها في المجمع الرئاسي قبل أن تتحول بصورة نهائية الى مقر القيادة العامة للقوات المسلحة الإيرانية، بناء على أمر مباشر من المرشد الأعلى والرئيس الإيراني السابق أحمد نجاد، الأمر الذي ينبئ عن حصول تحول في وظيفتها، وارتباطها بأنشطة القوات المسلحة الإيرانية، وبشقها الدفاعي على التحديد (*BBC,2013*).

وسعى النظام الإيراني، شيئاً فشيئاً الى توسيع نطاق الدور الذي تمارسه هذه المنظمة على صعيد حماية البنية التحتية لالفضاء السيبراني الإيراني، بعد أن التصقت الكثير من العقد السيبرانية لالفضاء السيبراني مع مشاريعها برنامجها النووية، ومفاصل استراتيجية أخرى للبلاد فعمّقت حضور الصبغة العسكرية في الكثير من مهامها، الأمر الذي دفع

---

[164] . ترجمت المنظمة هذه الخطاطة على أرض الواقع، من خلال إنشاء مجموعة مكاتب، لقيادة أنشطة الفضاء السيبراني في عموم إيران، منذ بدايات شهر أكتوبر 2011، واوكلت لها مهمة التخطيط وترجمة هذه الخطة على أرض الواقع، والمباشرة بالوقت ذاته في ترسيخ حصانة رقمية للدفاع عن البنية التحتية في إيران، عبر مراكز القيادة التي باتت حاضرة في جميع المحافظات الإيرانية.

[165] . راجع التصريح على الموقع: *http://theunhivedmind.com/wordpress3/passive-defense-organization-of-iran-to-hold-nationwide-cyber-maneuver/*

بقائدها الى وضع حدود مهامها بتصريحه الذي أطلقه عام 2014 وقال فيه: إن عملية الدفاع المدني تعني أضحت تعني لنا سلسلة من الممارسات التي تروم التعرّف على الأعداء، والتهيؤ لمواجهة أفعالهم العدوانية، وتحذيرهم، ومجالدتهم، والاستمرار بدرء أخطارهم لحين ضمان النصر عليهم[166].

وقد استمرت هذه المنظمة بحشد وتجنيد الموارد البشرية من قراصنة المعلومات الموجودين في إيران لتعزيز قدراتها السيبرانية، حيث دعا غلام رضا جليلي، رئيس مؤسسة المقاومة السلبية، خلال المؤتمر الثاني الذي عقدته مؤسسته خلال النصف الأول من عام 2011 ذوي النوايا الحسنة من قراصنة المعلومات، الذين ينتمون الى روح الثورة الإسلامية، ببذل كل ما في وسعهم من خلال تسخير قدراتهم وخبراتهم لدعم أهداف الجمهورية الإسلامية وتعزيز سلطانها السيبراني(*MAI,2011*).

4 . 3 . 3 . شرطة فضاء إيران السيبراني *FATA*:

شكّلت فصائل شرطة فضاء إيران السيبراني *FATA* استجابة لتنامي أنشطة المعارضة الإيرانية في فضاء الفيض السيبراني، اثناء حملة الانتخابات الرئاسية في عام 2009، بينما برّرت الحكومة ولادة هذا التشكيل لمكافحة الجرائم التي ترتكب في الفضاء السيبراني (*BBC,2013*). وتضم مؤسسة شرطة فضاء إيران السيبراني مجموعة من الوحدات الملحقة بمركزها الرئيسي، منها مراكز التدريب التي تنهض بمهمة تطوير مهارات وقدرات العاملين في مراكز الشرطة السيبرانية المنتشرة في عموم البلاد، ووحدات لمراقبة جميع الأنشطة التي تمارس على مواقع الويب والمدونات السيبرانية، ومتابعة المنشورات التي تطرح على صفحات شبكات التواصل الاجتماعي والتي يشكّل بعضها تهديداً امنياً للنظام (*SMO,2013,b*).

ومع مرور الوقت أوكلت لهذا التشكيل الأمني مهام ذات صبغة سياسية، والتي يعدّها النظام جزءاً لا يتجزأ من سياسته في الدفاع عن حياض الفضاء السيبراني من الهجمات والتهديدات التي يمارسها المعارضون للنظام الايراني، من داخل إيران وخارجها، فأضيفت الى قائمة مهام، مهمة جديدة أطلق عليها "مهمة درء التهديدات الأمنية السياسية والأمنية"(*IHRO,2014*).

فالتزم الجهاز بتحديد مواطن الضعف والثغرات السيبرانية المقيمة في النسيج الشبكاتي لالفضاء السيبراني الإيراني للمواقع الحكومية، والسعي الى سد هذه الثغرات، بالإضافة الى ممارسة عملية تقطير المحتوى السيبراني للمواقع التي لا تتوافق مع أخلاقيات الثورة الإسلامية، وحجب مواقع البريد الالكتروني المعارضة (*Wheeler,2013*).

وقد أعلنت إدارة شرطة فضاء إيران السيبراني أنها تستخدم تطبيقاً برمجياً أطلق عليه اسم العنكبوت الأسود *Black Spider* والذي يقوم بالتحرّي عن مواقع التواصل الاجتماعي *Facebook* المشبوهة وإلقاء القبض على أصحابها الذين يطلقون منشورات تعارض خطاطة النظام أو لا تتوافق مع المنظومة العقدية للثورة الإسلامية (*Crowdstrike,2015*).

وقد صرّح أكثر من مسؤول أن الشركة الإيرانية التي انتجت هذا البرنامج قد نجحت في إنتاج نسخ محدّثة منه قادرة على ترشيح مادة المحتوى المطروح في تطبيقات أخرى تستوطن في منصة تطبيقات التواصل الاجتماعي، وبرمجيات تواصلية تستخدم في الهواتف الذكية مثل تطبيق: *Viber*، *WhatsApp* وغيرها (*Crowdstrike,2015*).

وبهذا يمكننا القول أن هذا التشكيل الأمني قد التحق شيئاً فشيئاً ضمن منظومة الدفاع السيبراني في إيران، وأصبح يمارس مهام ذات صلة بالدفاع عن المواقع المحلية (حكومية، أو خاصة) ضد الهجمات المحتملة من قراصنة المعلومات

---

[166] . راجع التصريح على الموقع: *http://www.criticalthreats.org/iran-news-round-october-31-2014*

المحليين، بالإضافة الى تتبع موارد التهديدات أو الهجمات، أو المحتوى السيبراني لخطاب المعارضة، أو الجهات التي تناوئ النظام الإيراني في أي ميدان من الميادين ذات الصلة بالواقع الإيراني.

4 . 3 . 4 . مراكز متنوعة للدفاع عن الفضاء السيبراني الإيراني:

نتيجة لانبساط استخدام تقنيات المعلومات والاتصالات على مساحة واسعة من الأنشطة التي تسري في مجتمع المعلومات والمعرفة الإيراني، وتزايد مستوى الهاجس الأمني لدى النظام الأمني على المستويين الحكومي والفردي، فقد تكاثر عديد مراكز الدفاع التي خصصت للدفاع عن مراكز المعلومات ضد الاختراقات والهجمات المحتملة، مع تنوّع اهتمامات هذه المراكز بتفاصيل المهام الأمنية التي تمارسها لضمان الحصانة الأمنية المطلوبة.

ويلاحظ أن بعضها لا يعدو عن كونه وحدة صغيرة ملحقة بنشاط محدد في إحدى المؤسسات أو الشركات، بينما يرتقي بعضها الى مستوى مهام ذات صلة بنشاط قطاع كبير، أو على مستوى الأمن القومي. وتمارس هذه الكيانات دورها على التوازي مع الأدوار التي تمارسها الكيانات العملاقة التي وفر لها النظام الإيراني دعماً مالياً ولوجستياً مميزاً، وبدعم توفره المؤسسات التي ترتبط بها، لضمان سد أكبر حجم ممكن من الثغرات التي توفر لخصوم إيران فرصة الولوج الى جزء من أجزاء فضائها السيبراني الفسيح.

فعلى سبيل المثال أنشئت في نهاية عام 2011 أنشئت مجموعة مراكز كلفت بمهمة درء المخاطر والدفاع عن الفضاء السيبراني، فاوكلت اليها مهمة درء المخاطر المصاحبة للديدان السيبرانية الخبيثة *Worms* ومنعها من اختراق نظم المعلومات، أو استراق البيانات والمعلومات المهمة من الشبكات السيبرانية التي تتمتع بمستوى عال من السرية والأمن السيبراني، والتي تضم كل من: جميع منظومات برامج إيران النووي، ووحدات إنتاج الطاقة، ومراكز البيانات، والمصارف[167].

كذلك شهدت مؤسسة الجيش الإيراني ولادة مراكز خاصة لفضاء معلومات الجيش الإيراني *Cyber Headquarters Of Iranian Army* والتي وضعت نصب أعينها فرصة نشر قيم الثورة الإسلامية في محيط المعلومات العولمي. وذهب قائد هذه المراكز، بيهروز أسباطي، في تصريح له لإحدى القنوات الإخبارية الإيرانية *Mersadnews.ir* بتاريخ 20 مارس 2013 أن البيئة الافتراضية لالفضاء السيبراني توفر مناخاً مناسباً لتوطئة ظهور الامام المهدي، بعد أن وقع العالم الغربي في فخ العولمة، وسيادة المادية، وضياع القيم، فترك المجال مفتوحاً أمام من يريدون ترسيخ الحضور الإسلامي بثقافته وقيمه في عالم بات يفتقر الى القيم. وقد بالغ في مقولته عندما عد أن عصر المعلومات الافتراضي هو عصر ظهور إمام الزمان (على حد تعبيره) وأن إيران حريصة على أن تمارس دوراً مهماً لعملية التمهيد من خلال تطوير قدراتها السيبرانية الى مستوى يتوافق مع هذه المرحلة المهمة في تاريخ البشرية، بحسب تصريحه (*Mansharof,2013*).

ويضاف الى ذلك أن هناك الكثير من المشاريع التي تولد في منظومة الدفاع الأمني الإيراني لتلبية حاجات آنية، وتسهم في سد الثغرات الأمنية في الفضاء السيبراني الإيراني، والتي يطويها النسيان بعد انتهاء المهام التي كانت مبرراً لولادتها، منها مشروع *Gerdab* الذي قامت مؤسسة الحرس الثوري الإيراني بتنفيذه للكشف عن هوية الناشطين السيبرانيين، والشبكات المعارضة التي ينتمون إليها للحد من أنشطتهم وخطاباتهم السيبرانية المناهضة للنظام قبل، وأثناء، وبعيد

---

[167] . راجع المصدر على الموقع: *http://theunhivedmind.com/wordpress3/passive-defense-organization-of-iran-to-hold-nationwide-cyber-maneuver/*

حملة الانتخابات الرئاسية لعام 2009 وبتنسيق مباشر مع منظمة الباسيج التي أوكلت إليها جميع تفاصيل إدارة فعاليات هذا المشروع[168].

ونقر بصعوبة الإحاطة بهوية ومهام هذه الوحدات الأمنية والمراكز، والتي أضحت بعد هجمات الفايروس الخبيث *Stuxnet* ممارسة ضرورية لا يستغنى عنها في جلّ قطاعات المعلومات والاتصالات في إيران، والتي بدأت تتناسل خلال العقد الأخير مع توسع دائرة مهامها وتكاثر ارتباطاتها المتنوعة مع الهيكلة الهرمية للنظام الإيراني ومؤسساته الأمنية المتعددة.

4 . 3 . 5 . مركز مهر لفرق الاستجابة الأمنية لحوادث الحواسب:

في بداية عام 2014، أنشأت وزارة تقنية المعلومات والاتصالات في إيران، وتحت مظلة مؤسسة إيران لتقنية المعلومات مركز مهر *MAHER* للنهوض بمهام فرق الاستجابة الأمنية لحوادث الحواسب *Computer Security Incident Response Teams (CSIRT)* والتعامل (وفق المعايير والممارسات الدولية) مع التهديدات والهجمات السيبرانية المتكاثرة على البنى التحتية للمعلومات والاتصالات والمواقع المهمة والحيوية في إيران، وإيجاد الحلول لمنع تكرارها من خلال الارتقاء بالحصانة الأمنية، وغيرها من الإجراءات المعتمدة بهذا المضمار[169].

وقد حدد مجال عمل المركز بجميع المؤسسات والشركات الحكومية التي تعمل بمعية وزارة تقنية المعلومات والاتصالات الإيرانية، بينما حصر عملها مع شركات القطاع الخاص التي رخصت أنشطتها وفق معايير الوزارة ذاتها. بينما جعل استخدام المحتوى السيبراني للموقع لجميع المستخدمين الإيرانيين من خلال اتاحة مادة المحتوى للاستخدام الشعبي.

وضم الهيكل التنظيمي للمركز مجموعة من الفرق المتخصصة بتقنية المعلومات والاتصالات وأمن نظم المعلومات والشبكات، شملت كل من:

- فريق تحليل الهجمات والتهديدات السيبرانية وتقييم آثارها المحتملة.
- فريق تحديث قواعد البيانات والمراقبة الآنية.
- فريق الكشف عن الاختراقات والاستجابة للحوادث والتهديدات السيبرانية.
- فريق تنسيق إجراءات الاستجابة للحوادث والتهديدات الأمنية.
- فريق الدعم التقني وصيانة النسيج الشبكاتي ونظم المعلومات.

وقد وحّدت عمل هذه الفرق مجتمعة ضمن إدارة موحدة في مركز مهر، لضمان التعامل السريع مع التهديدات والحوادث الأمنية المحتملة، وبإشراف مباشر من قبل وزارة تقنية المعلومات والاتصالات.

وأنيطت بالمركز مجموعة متنوعة من المهام تضمنت: إجراء تقييم ميداني للجوانب الأمنية التي تتسم بها نظم المعلومات والنسيج الشبكاتي الإيراني، والعمل على تشكيل فرق دعم في مؤسسات وشركات الوزارة ذاتها لتعزيز ودعم كوادر المركز مع توسيع رقعة التعامل الآني مع التهديدات والحوادث الأمنية، مع السعي لنيل عضوية الفرق الآسيوية والعولمية التي تمارس المهام ذاتها لكسب المزيد من الخبرات والمهارات من خلال التواصل والتعاون المشترك.

[168] . عكفت الفصائل السيبرانية في جيش فضاء إيران السيبراني *ICA* على معالجة الفيض السيبراني الذي أطلقه الناشطون الإيرانيون في فضاء تطبيقات التواصل الاجتماعي، ونجحت في الكشف عن هوية هؤلاء الناشطين مع توفير بيانات تفصيلية دعمت منظمة الباسيج وبالتنسيق مع منظمة الدفاع السلبي المتمثلة بشرطة فضاء إيران السيبراني في عملية إلقاء القبض على الناشطين الذين شاركوا بعملية إنشاء أكثر من 90 موقعاً ينطق باللغة الفارسية، وينشر مادة تخالف خطاطة الدين الإسلامي، وثوابته الأخلاقية. وقد هرعت التشكيلات المعنية بغلق هذه المواقع، وتقديم الناشطين للقضاء الإيراني.

[169] . موقع المركز: https://www.certcc.ir/.

وقد حقق مركز مهر نجاحات مهمة، رغم عدم مرور بضعة سنوات على إنشائه، فساهم وللمرة الأولى ضمن الفريق العولمي لأمن المعلومات الذي عكف خبراؤه على تحليل معمارية الدودة الخبيثة *Flame* ونجح ببناء أداة لإزالة تأثيره على نظم المعلومات التي قد أصيبت بآفته الضارة، وكان للأداة التي ابتكرها المركز صدى كبير بين الشركات الأمنية في مختلف بلدان العالم (*Jackson,2012*).

ولم يقتصر طموح الإدارة السيبرانية في إيران على تنشيط الدور الذي يساهمه هذا المركز في حماية مواقع مؤسساتها من الهجمات، واتخاذ التدابير اللازمة لتجاوز تأثيراته المحتملة، فحاولت مد أنشطته على مساحة تجاوزت حدود البلاد.

فبدأت كوادر المركز بالتواصل مع الشركات المتخصصة بمكافحة الفايروسات والديدان الخبيثة، وزودتهم بتحليل لمعمارية الدودة الخبيثة *Flame* التي استهدفت مؤسساتها، وذلك لدعم أنشطتهم في إنتاج أداة للكشف عنه، ومعالجته بطريقة آمنة، إضافة الى توفير هذه الأداة على موقع المركز لمن يروم الحصول عليها.

4 . 3 . 6 . مركز العمليات الأمنية للبيئة الصناعية:

أنشئ مركز العمليات الأمنية للبيئة الصناعية *The Security Operations Center (SOC) for the Industrial Environment* في 13 نوفمبر عام 2013 لتوفير حصانة أمنية للمنشآت الصناعية في عموم إيران من التهديدات والهجمات المحتملة على فضائها السيبراني المرتبط بالفضاء العولمي (*SMO,2013,b*).

ولترسيخ أمن المعلومات في القطاع الصناعي تعكف الكوادر التقنية والسيبرانية في هذا المركز على إنتاج مجموعة متنوعة من النظم البرمجية الأمنية، وبعض الأدوات السيبرانية التي تدعم أمن عتاد النسيج الشبكاتي الداعم للأنشطة الصناعية في عموم هذا القطاع بالبلاد، وتدافع عن البنية التحتية للمعلومات والاتصالات إزاء التهديدات والهجمات المحتملة.

4 . 3 . 7 . لجنة تحديد المواقع غير المرخصة:

بالإضافة الى ما ذكر من مؤسسات تنتمي بصورة مباشرة الى الإدارة العليا للدفاع فإن هناك مؤسسات تقدّم خدماتها الى منظومة الدفاع والردع السيبراني، إلا أنها تمارس دوراً غير مباشر في عملية ترسيخ الأمن السيبراني ودرء مخاطر الهجمات اللينة التي تمارس ضد النظام وخطاطته. منها هيئة تمييز مواقع الويب ـ غير المرخصة *Committee to Identify Unauthorized Websites* والتي ترتبط بالمجلس الأعلى للثورة الثقافية، والتي تقوم بمهمة التنقير عن المواقع التي تطرح مضامين تناهض خطاطة الثورة الإسلامية في إيران، وتعارض النظام وتوجهاته.

وتسهم مثل هذه الهيئة في إيصاد البوابات التي يتسلل من خلالها خطابات الثورة اللينة المناهضة للنظام، والتي يعدّها جزءاً لا يتجزأ من سياسته في درء التهديدات الناعمة عن المحيط الثقافي للمواطنين الإيرانيين.

وتساهم لجنة تحديد مواقع الانترنيت المحظورة *Committee to Identify Unauthorized Internet Sites* في ممارسة جزء محدود من أنشطة الدفاع عن حياض الأمن السيبراني في إيران عن طريق تتبع آثار وعنونة المواقع التي تخالف ثقافة الثورة الإسلامية بإيران، أو تطرح محتوى سياسي أو عقدي مناهض.

ولدت هذه اللجنة استجابة لتوجيهات المرشد الأعلى للثورة وألحق بها مجموعة من قيادات النظام الإيراني لدعم قرارتها، ومن أعضاء هذه اللجنة: النائب العام، ووزراء كل من وزارة: الثقافة، والمخابرات، وتقنية المعلومات والاتصالات، والعلوم والتقنية، والقائد العام لقوات الشرطة، ومدير الإذاعة والتلفزيون الإيراني، وشخصيات أخرى.

ولم تقتصر عملية حظر المواقع على مواقع الجهات المعارضة، أو الشركات الإيرانية التي لا تلتزم بطرح المضامين التي تتوافق مع خطاطة النظام، بل هناك كثير من الوقائع التي تشير الى أن هذه اللجنة قد مارست عملية الحظر على

المواقع الرسمية لشخصيات مرموقة في النظام، مثل هاشمي رفسنجاني بعد أن طرح مادة عدّت مخالفة للمعايير المعتمدة بالسماح للمواقع الالكترونية.

ولا تتوفر أية ادلة حول ممارسات أخرى لهذه اللجنة خارج نطاق المهام الموكلة لها، وهي حماية محتوى الفضاء السيبراني الإيراني من أي محتوى مخالف لتوجهات النظام وتطلعاته السياسية، والعقدية، والثقافية.

4 . 4 . كيانات الدفاع والردع السيبراني:

لا ينكر العاملون في مجال حروب الفضاء السيبراني السمات المعقدة التي تتسم بها هيكلة مؤسسة الدفاع والردع السيبراني الإيرانية، بحيث يصعب على الكثير تحليل معماريتها، والكشف عن هوية العناصر المساهمة في تشكيل هذه المعمارية التي تتميز بتلاحم المؤسسات الملحقة بها، مع تشابك خيوط الارتباط التي تجمع بين عناصر نسيجها المتنوعة بحيث أن الكثير من الجهات المشاركة في تنفيذ مهامها قد لا تتوفر لديها صورة واضحة المعالم عن طبيعة الدور الذي تمارسه ضمن الاطار الكلي لممارسات الدفاع والردع السيبراني لهذه المؤسسة التي استغلق على الكثير سبر جوهرها (*Wheeler,2013*).

تتألف هيكلة القوة السيبرانية الإيرانية من مجموعة الفصائل ووحدات الدفاع والردع السيبراني التي تعمل مع (*HP,2014,a*):

- ✓ منظمة الدفاع المدني الإيرانية[170].
- ✓ مؤسسة الحرس الثوري الإيراني *Pasdaran*.
- ✓ مؤسسة الباسيج شبه العسكرية.

وقد أوكلت مهمة الدفاع عن بيضة إيران السيبرانية، وكياناتها المؤسسية الى منظمة الدفاع المدني لكي تتوافق مع القدرات والخبرات التي تتمتع بها فصائل هذه المنظمة والتي تعكف على حماية الموجودات الشبكاتية بالبلاد تجاه مختلف أشكال التهديدات المحتملة.

ويتكون الهيكل التنظيمي للوحدات السيبرانية في هذه المنظمة من قيادة دفاع الفضاء السيبراني ووحدة *Gerdab* التي أوكلت إليها مسؤولية تحديد هوية وتتبع وتخويف المعارضة خلال أحداث الحملة الانتخابية الرئاسية عام 2009.

أما الحرس الثوري الإيراني فتدين له بالانتماء والولاء، مؤسسة الباسيج (شبه العسكرية) التي تنهض بمهمة فرض الخطاطة الثقافية والعقدي للثورة الإسلامية، وينبثق عنها مجلس الفضاء السيبراني في منظمة الباسيج *Basij Cyber Council*، وكذلك شرطة الفضاء السيبراني *FATA*.

ويتمتع مجلس الفضاء السيبراني بمهارات واسعة في قطاع المعلومات والاتصالات تشمل:

- تشويش وخلخلة أداء قنوات بث الأقمار الاصطناعية.
- مراقبة وممارسة الحظر وتضييق الخناق على فضاء الوسائط المتعددة والأخبار التي تستخدمها المعارضة لمناهضة النظام وأنصاره.
- ممارسة عمليات الحظر والمراقبة على فضاء الانترنيت وبالخصوص الفيض السيبراني المسافر في تطبيقات شبكات التواصل الاجتماعي.

[170] . عمدنا الى ذكر منظمة الدفاع السلبي في هذا المحور ثانية لأن ثمة تغيّر قد بدأت علائمه بالظهور بعد الهجمات التي استهدفت أجهزة الطرد المركزي بحيث بدأت المنظمة باستقطاب قراصنة للمعلومات لم يعد عملهم مقتصراً على عملية الدفاع السلبي، وإنما تطور فشمل عمليات الدفاع والردع السيبراني، من أجل هذا اقتضى التنويه.

- ممارسة الدعاية المضادة وتشويش مادة الخطاب المعارض الذي يطرح على مواقع الانترنيت.
- تقطير مادة المحتوى السيبراني المطروح على مواقع الويب لتغييب الخطاب المناهض للنظام ومؤسساته المختلفة.

ويترأس مجلس الباسيج لالفضاء السيبراني الأستاذ الدكتور حسان عباسي، أحد الأساتذة من الجامعات الإيرانية، والذي مارس دوراً مهماً في جذب وتجنيد الكفاءات العلمية في مجال المعلومات والاتصالات، والطلبة الذين يتمتعون بمهارات مميزة في مضمار القرصنة السيبرانية ضمن الجامعات الحكومية، ومراكز بحوث وحاضنات تقنيات المعلومات التي تتلقى دعماً مباشراً من الإدارة الحكومية. وقد أسهم الخطاب الذي وجهه المرشد الأعلى للثورة الإسلامي، علي خامنئي في شهر شباط عام 2014 الى الاتحاد الإسلامي لطلبة الجامعة المستقلة، بالتهيؤ للمشاركة الفاعلة في أنشطة حرب المعلومات لأنها جزء لا يتجزأ من واجبهم الوطني تجاه إيران، والعقدي تجاه عقيدتهم الإسلامية الراسخة (*HP,2014,a*).

أما شرطة الفضاء السيبراني فتنهض بمهمة فرض قانون وتشريعات الفضاء السيبراني التي أقرها المجلس الإيراني، وتوطيد هيمنة النظام على الفضاء ودرء عمليات تغلغل الخطاب المعادي، وردع من تسوّل له نفسه ممارسة الجرائم السيبرانية ضد الأفراد، ومؤسسات الدولة، والقطاع الخاص.

وقد حرص النظام على تشكيل قوة رقمية ـ إيرانية رادعة على التوازي مع القوة التي عكف على تهيئتها لممارسة العمليات الدفاعية عن بيضة البلاد السيبرانية. واستمر بالنهج ذاته، في تنويع موارد القوة الرادعة بحيث لم تقتصر على المؤسسات العسكرية والأمنية، فألحق بها جيش إيران السيبراني الذي يعمل بمعية الحرس الثوري الإيراني، والفصائل السيبرانية الملتحقة مع منظمة الباسيج، إضافة الى تجنيد الكثير من مجاميع القرصنة السيبرانية العريقة، كونها باتت تحمل واجهة شركات أمنية في عموم البلاد، بالإضافة الى تجنيد أفراد متفرقين من القراصنة المتميزين، والتي عكفت مؤسسة الحرس الثوري، والباسيج، وشرطة إيران السيبرانية على تتبع أنشطتهم، وملاحقتهم، وعقد اتفاقات غير معلنة، وتنسيق دائم لحضورهم في العمليات الهجومية التي يروم النظام مباشرتها ضد أهداف استراتيجية تستوطن في النسيج الشبكاتي للدول المناهضة للنظام، فتعتمد مشورتهم، ويستأنس بخبرتهم في تحديد طبيعة الفجوات الأمنية الموجودة، وتحديد النهج الأمثل لتحقيق تأثيرات كبيرة.

لقد أسهم التنوّع في انتقاء الموارد البشرية، وتوظيف مساحة واسعة من البنية التحتية لأكثر من مؤسسة حكومية، وشركات أمنية، متعددة الوظائف، مما أسهم في تعميق خبراتها، فأضحت هجماتها أشدّ تأثيراً، مع نضوج خططها ووضوح أهدافها نتيجة لتمرير خططها عبر أكثر من قناة، وتوالي مراجعاتها من خلال أكثر ميدان من ميادين التخصص والخبرة.

4 . 4 . 1 . جيش إيران السيبراني *Iran Cyber Army (ICA)*

طرحت مؤسسة الحرس الثوري الإيراني فكرة تشكيل فصيل رقمي يكون نواة لجيش فضاء إيران السيبراني في بدايات عام 2005. وقد ولد هذا المقترح نتيجة لتنامي القناعة لدى المؤسسات الأمنية والاستخبارية في إيران بأهمية استثمار قدرات قراصنة المعلومات الإيرانيين وتوجيهها كقوة ضاربة تدافع عن الكيانات السيبرانية في الفضاء السيبراني الإيراني، أو توجيه هجماتهم نحو أهداف تعود الى المعارضة الإيرانية، والدول التي تناهض النظام.

أجبر الحرس الثوري الإيراني على ترجمة رؤيته (بصدد تشكيل قوة رقمية ضاربة) الى تشكيل حقيقي على أرض الواقع عندما عصفت بالبلاد الاضطرابات التي صاحبت الحملة الانتخابية الرئاسية لعام 2009. بعد أن أقبلت المعارضة

بقوة، وبتنسيق عال، على توظيف جميع القدرات الكامنة في تطبيقات شبكات التواصل الاجتماعي لإذكاء صوت المعارضة ضد التجاوزات التي حصلت أثناء تلك الحملة الانتخابية. بدأت التغريدات السيبرانية بالسفر بين الهواتف المحمولة، وأعلن عن التجاوزات من خلال السيل الجارف من الصور والمقاطع الفيديوية، ووثقت كل حركة وسكنة مورست لمواجهة المعارضة عبر تطبيقات التواصل الاجتماعي، الأمر الذي أوقع النظام في حرج شديد أمام الرأي العام العالمي (*Shakarian,et.,al.,2013*).

لقد أيقن الحرس الثوري أن وجود القوة السيبرانية أصبح لزاماً لحماية الثورة ومكتسباتها، ودرء الانحدار المحتمل نحو ارتفاع أصوات المعارضة الى مستوى لا يمكن التعامل معه بسهولة، كما أن الخطاب المعارض قد نجح من خلال حملته السيبرانية عبر الوسائط المنفتحة على الجميع في كسب أصوات إضافية دعمت توجهات المعارضة المعتدلة قبالة الخطاب الذي صدع به المحافظون وأنصارهم.

لم تتسم البدايات بحضور خطة واضحة فكل ما أراده الحرس الثوري من قراصنة المعلومات الذين التحقوا بفصيله السيبراني (سواء نتيجة اقتناع أو بفعل الإكراه مقابل بعض التسهيلات) هو إيقاف مد الخطاب المعارض على صفحات مواقع التواصل الاجتماعي، فبدأت حملة شرسة على تطبيقات منصات التواصل، نشب عنها توقف موقع *Twitter*[171]، ثم توالت هجمات الفصيل الجديد على مواقع الحركة الخضراء ـ المعارضة فأوقفتها عن العمل نتيجة إغراقها بسيل من النبضات السيبرانية، و / أو أورثت المحتوى خللاً شوه مادة الخطاب المطروح على صفحاتها. ثم عكف القراصنة المستأجرون على التنقير عن هوية أصحاب الصوت المعارض فجمعوا صورهم، وبياناتهم الشخصية، ووضعوها في متناول الحراس الثوري، والباسيج، والبوليس السيبراني لكي تبدأ عملية ملاحقتهم وتقديمهم الى العدالة بتهمة الاخلال بأمن البلاد ومحاولة تقويض النظام.

وبدأت الإدارات التخطيطية في الحرس الثوري بالتحضير لصياغة وتشكيل هوية جيش فضاء إيران السيبراني لكي ترتكز أركانه الى أرضية صلبة، وتتوسع دائرة واجباته ومهامه بما يخدم خطاطة الثورة الإسلامية في إيران. فأصبحت هذه التسمية تؤشر نحو تشكيل لقوة رقمية ضاربة لتلبية الأنشطة الدفاعية الهجومية للدولة في فضاء الفيض السيبراني، تكلّف بهجمات معلوماتية ضد مواقع الويب تعود لأي جهة محلية تناوئ خطاطة النظام، إضافة الى ممارسة عمليات القرصنة والتجسس السيبراني على مواقع النظم والدول المناهضة للثورة الإسلامية. ومنذ ذلك التاريخ حرص الحرس الثوري الإيراني، والباسيج على جذب وتجنيد صفوة قراصنة المعلومات في البلاد، من خلال التنسيق مع إدارات الشركات الأمنية، أو بالاتصال المباشر مع من يثبت لديهم أن له ممارسات قرصنة يعلن عنها في مواقع ومنتديات القرصنة السيبرانية المحلية أو الدولية.

تعد مجموعة قراصنة *Ashiyane* من أوائل مجاميع القرصنة المحلية التحاقاً بالمؤسسة الحكومية وممارسة سلسلة من الهجمات وعمليات القرصنة لصالح النظام الإيراني. وقد أعلنت وسائل الاعلام الحكومية عن هذه الهجمات التي نالت خصوم الثورة الإسلامية، فنشر أكثر من خبر ومقال في كل من: الصوت والرؤية، وكيهان، ووكالة الأخبار الإيرانية (*Rezvaniyeh,2010*).

ويذهب بعض الباحثين الى تأكيد قيام المؤسسات الأمنية الإيرانية، مثل: الحرس الثوري الإيراني، والباسيج، ومنظمة الدفاع المدني، وشرطة إيران السيبرانية بعقد صفقات، غير معلنة، مع قراصنة المعلومات الذين قد وقعوا في قبضة

[171] . نجح قراصنة المعلومات في جيش فضاء إيران السيبراني باستبدال الصفحة الرئيسة لموقع التغريد السيبراني *Twitter* بصفحة كتب عليه "هذه الصفحة اخترقت بواسطة جيش فضاء إيران السيبراني".

القضاء، بسبب ممارستهم لجرائم قرصنة معلوماتية، لتخفيف الأحكام عنهم، أو إطلاق سراحهم مقابل العمل لصالح النظام وشن هجمات شرسة ضد أهداف تنتخبها إدارة الفصائل والميليشيات السيبرانية المرتبطة بهذه المؤسسات (*Rezvaniyeh,2010*).

وقد توطدت العلاقة بين الطرفين، وسادها نوع من التوافق وتطابق التوجهات، بعد أن شعرت مجاميع قراصنة المعلومات بالهدنة التي عقدها النظام معهم، وغضّ الطرف عن بعض نشاطاتهم التي قد تعرضهم للمساءلة القضائية، أو الملاحقة الأمنية، وتطورت هذه العلاقة شيئاً فشيئاً فبدأت مجاميع القراصنة، وشركاتها الأمنية في توفير خدمات متنوعة للقراصنة المجندين في المؤسسات الحكومية، بدءاً بتدريب هذه الكوادر والارتقاء بمستوى مهاراتها، وتوفير المشورة بخصوص الثغرات الأمنية التي يمكن استثمارها في تمرير الهجمة نحو مواقع الجهات المناوئة للنظام، وتوفير الموارد اللازمة لإنجاح الهجمة، سواء كانت هذه الموارد تطبيقات قرصنة برمجية، أو مشورة فنية لتوجيه مسارات فصائل القرصنة الحكومية، أو حتى المشاركة معهم بكوادر خبيرة من هذه الشركات لضمان نجاح الهجمة، وتعميق مستوى تأثيراتها الضارة في مواقع الخصوم (*Rezvaniyeh,2010*).

إضافة الى ذلك باشرت الإدارة الحكومية بتوفير جميع أشكال الدعم والتسهيلات المالية واللوجستية (لهذه الشركات) لاستيراد ما تحتاج اليه من ادوات رقمية، وبرمجيات تطبيقية تدعم أنشطة القرصنة، لتجاوز عقبة الحظر التقني الذي فرضته الولايات المتحدة على النظام الإيراني، فتوفر بصورة غير مباشرة، لفرق القرصنة الحكومية، تقنيات وأدوات متطورة تسهم في دعم قدراتهم وترفع من مستويات سلطانهم السيبراني.

ورغم كل هذه المعلومات عن بعض مفردات التحالف بين الطرفين لازال هناك الكثير من الغموض الذي يلف تفاصيل وثيقة التوافق التي عقدتها المؤسسات الأمنية الإيرانية مع قراصنة المعلومات، أو الشركات الأمنية الإيرانية، وهل أن الاتفاق قد تضمن عمل قراصنة المعلومات بصورة كلية تحت مظلة هذه المؤسسات، أم ان الاتفاق قد أبرم حول تفرّغ جزئي لقراصنة المعلومات وكوادر شركاتها بالتنسيق مع هذه المؤسسات لشنّ هجمات محددة تلتزم بتوجيهاتها، وبحسب معطيات كل حالة من الحالات، مع توفير معلومات دقيقة عن الثغرات الأمنية في نظم معلومات خصوم إيران.

وقد برز اسم جيش فضاء إيران السيبراني على سطح الأحداث عند نهاية عام 2009 عندما انتشر خبر حصول هجمة معلوماتية شرسة على موقع الصوت الأخضر، والذي كان يعبر عن صوت المعارضة الإيرانية أبان الحملة الانتخابية الرئاسية في إيران، ومنذ ذلك التاريخ توالت الهجمات كتائب هذا الجيش على أهداف رقمية تتوزع بأماكن متباعدة في الفضاء السيبراني ـ العولمي (*Azani,2015*).

وبات التشكيل عبارة عن تجمع لمجموعة من صفوة قراصنة المعلومات الإيراني، دون أن تكون له صفة رسمية ضمن الهرم المؤسسي للإدارات الحكومية في البلاد. لذا ذهب البعض الى عده ميلشيا رقمية جنّد أفرادها بإشراف مباشر من قبل مؤسسة الحرس الثوري الإيراني، ومؤسسة الباسيج لممارسة مهام سرية تتعلق بقرصنة مواقع المعارضة داخل البلاد، ومناهضي خطاطة الثورة الإسلامية وخصومها خارج البلاد، دون أن يمنح النظام لخصومه فرصة الصاق تهمة التخطيط أو مباشرة الهجمات ضد هذه الجهات(*HITCON,2013*).

ورغم مرور بضعة سنوات على ولادة هذا التشكيل العسكري ـ السيبراني، فلا زال الغموض يلف هويته من جوانب عدة، سواء من حيث هوية الجهة التي يرتبط بها أفراده، وهل أن أفراد هذا الجيش الافتراضي ينتمون الى المؤسسة العسكرية، أم الى مؤسسة الحرس الثوري الإيراني، أم الى جهة أخرى لم يعلن عنها. كذلك هل أن هذه الفصائل قد

كلفت بالدفاع عن الحياض السيبرانية لإيران، أم أنها قد شكّلت لتكون الذراع السيبراني الضارب في أعماق أهداف خصوم إيران وأعدائها التقليديين؟.

بيد أن المراجعة المتأنية لسجل الهجمات (التي أعلن عنها جيش فضاء إيران السيبراني) تكاد تفصح بجلاء أن ممارسات فصائله تعد ترجمة مباشرة لخطاطة النظام الإيراني التي قد التزم بها الحرس الثوري الإيراني لدرء الأخطار المحدقة بالثورة الإسلامية التي يعد نفسه المسؤول المباشر عن حماية مكتسباتها.

ويلاحظ وجود تباين شديد وتعارض في مضامين تصريحات قيادات الحرس الثوري الإيراني لارتباط جيش فضاء إيران السيبراني بهذه المؤسسة، وبين ناف لوجود أي صلة بين هذه الفصائل السيبرانية بالمؤسسة ذاتها. فبالرغم من تأكيد غلام ميرزا جليلي، أحد كبار قادة الحرس الثوري، على أهمية وجود قوة ردع رقمية لدرء الهجمات المتكررة على البلاد، وكف أنشطة المعارضة الإيرانية، إلا أنه لم يفصح عن وجود أي علاقة مباشرة بين مؤسساته والجيش السيبراني الوليد في إيران، غير أنه رحب بوجود قراصنة معلومات إيرانيين يتطوعون لأداء هذه المهام الحيوية. بينما اعترف العقيد علي فضلي، أحد قادة الحرس في لقاء صحفي مع وكالة أخبار مهر بتاريخ 13 مارس 2010 أن هذا التشكيل موجود ضمن فصائل الحرس الثوري، وأن قطعات هذا الجيش تتألف من خبراء أكاديميين يعملون بمعية مؤسسة الباسيج، وطلبة متميزين من الجامعات الإيرانية، وطلبة متميزين بقدراتهم التقنية من فصول الحوزات العلمية، وميليشيات نسوية تعمل مع الباسيج (*IHRO,2014*).

من جهة أخرى فأننا نجد أنفسنا قبالة أكثر من عقبة مفاهيمية يشوبها تداخل واضح في تعريف هوية جيش فضاء إيران السيبراني، عندما نحاول تتبع توظيف اصطلاح الجيش السيبراني بتصريحات القيادات العليا في الثورة الإسلامية، والتي تجعل من هذه التسمية اصطلاحاً مشاعاً لوصف الفصائل السيبرانية المنتشرة بكثافة في البلاد، سواء اكانت هذه الفصائل تنتمي الى مؤسسة الباسيج، أو الى ميليشيات رقمية أخرى، مما يعيد الغموض ثانية حول هوية هذا الجيش، وحقيقة انتماءاته، وأمور أخرى تخص الكثير من تفاصيل الهجمات السيبرانية التي تمارس باسمه أو بمسميات قريبة منه (*IDC,2013*).

ولقد اتسع نطاق حضور جيش فضاء إيران السيبراني في عموم البلاد، وتهافت محترفو القرصنة من الشباب، والأكاديميين، والباحثين للالتحاق بصفوف فصائله المتكاثرة، وتعددت فروعه، حتى أصبح هناك مركزين من مراكزه في العاصمة طهران، وفق ما نقله مراسل الإذاعة البريطانية الناطقة باللغة الفارسية (*BBC,2013*).

وبالرغم من تناقض تصريحات المسؤولين إزاء مسألة الصلة القائمة بين الحرس الثوري الإيراني مع جيش فضاء إيران السيبراني، فمما لا شك فيه أن حضور الجيش السيبراني، ضمن تشكيلات الحرس الثوري الإيراني، أصبح امراً جلياً، وأن هذه القوة السيبرانية قد أصبحت تمثل جزءاً مهماً من أجزاء هذه المؤسسة، وأن التصريحات (في توافقها أو تناقضها) لم تعد كافية للتغطية على عدم انتمائه لمؤسسة الحرس الثوري، وائتمار فصائله بأوامر قياداتها، والتزامها بتحقيق غايات النظام وأجنداته السياسية والأمنية (*ONI,2013*).

ولا تكاد تعثر على معلومات دقيقة بصدد عديد الأفراد الملتحقين بفصائل هذا الجيش السيبراني، أو طبيعة هيكلة هذه المؤسسة العسكرية وارتباطاتها الوظيفية، ببقية المؤسسات الحكومية، كما أن البيانات التي تخص عديد أفراده لا زالت مشوشة، وتتأرجح بين عدد محدود من صفوة قراصنة المعلومات من المؤسسات الأمنية، وبعض مراكز البحث والمؤسسات الأكاديمية، وبين ما أفصحت به بعض الدراسات، والتي ذهبت الى أن عدد أفراد هذا الجيش قد ناهز 120 ألف مقاتل رقمي!.

إن هذا التناقض في تحديد هوية وعديد أفراد جيش إيران السيبراني قد نشب عن التكتم الشديد، وحرص النظام الإيراني على عدم الإفصاح عن هذه الأمور بقصد تشتيت جهود خصوم النظام لكشف النقاب عن هذه القوة الضاربة، تمهيداً لضربها، أو درء الأخطار المترتبة عن حضورها المكثّف في فضاء النزاع السيبراني.

ومما لا شك فيه أن سياسة تجنيد قراصنة المعلومات، وتنسيق أنشطتهم، وتوجيهها صوب تحقيق أهداف النظام ودعم خطابه السياسي والعقدي، قد اتسمت بنمط من نوع جديد اعتمد النسق الشبكي، بدلاً من الهيكلة الهرمية، الأمر الذي وفّر للقراصنة حرية التصرف، في ممارسة الهجمات والدفاع عن مواقع الويب التي ترتبط بمؤسسات النظام، دون التشديد على حضورهم والبدء بممارساتهم من خلال مواقع ذات صلة بأي مؤسسة من المؤسسات الحكومية. الأمر الذي أسهم في تشتيت وصلات الحضور السيبراني لممارسات القرصنة، بحيث بات من الصعوبة بمكان، تحديد هوية ممارسي هذه الهجمات، أو معرفة طبيعة الدوافع التي تكمن وراء هذه الهجمات، مع استبعاد وجود أية خيوط رابطة لأصحاب الهجمات مع مؤسسات النظام الإيراني[172].

وقد ذكرت بعض الدراسات التي عنيت ببيان العلاقة بين النظام الإيراني وقراصنة المعلومات، أن سياسة الحكومة قد تضمنت الكشف بصورة مسبقة عن الصفوة من قراصنة المعلومات بالبلاد، قبل أن تدفع بالمؤسسة الأمنية نحو الاتصال بهم وتخييرهم بين العمل مع جيش فضاء إيران الرقيم، أو التعرض للعقوبات القضائية. كما أن نهج التعامل مع القراصنة يعتمد مبدأ السرِّية التامة في التعاون مع قراصنة المعلومات وتنسيق الهجمات دون الإفصاح عنها، بحيث يعمل فريق القرصنة، بصورة منفصلة، ولا يوحي لبقية المشاركين طبيعة المهمة التي ينضوي فيها النشاط الذي مارسه (*Kokhreidze,2015*).

وذكر أحد قادة الحرس الثوري الإيراني المخضرمين، محسن سازيجارا، (والذي يقيم حالياً بالولايات المتحدة) أن مؤسسة الحرس الثوري قامت بتجنيد صفوة قراصنة المعلومات الإيرانيين مقابل أجور شهرية مغرية وصلت الى 10 آلاف دولار (وهو اجر يزيد بأكثر من 25 ضعفاً على متوسط الأجر الذي يمكن أن يحصل عليه من العمل في شركة أمنية). أما التقارير الأخيرة التي أشارت إليها دراسة الباحث (*Kokhreidze,2015*) فتؤكد أن كوادر جيش فضاء إيران السيبراني قد تنامى عديدها فبلغ عددهم أكثر من 2500 مقاتل رقمي، وأن الميزانية التشغيلية لهذا التشكيل باتت تكلف الإدارة الحكومية الإيرانية حوالي 80 مليون دولار سنوياً.

ويؤكد حقيقة الارتباط المباشر بين الجيش السيبراني والحرس الثوري، التصريح الذي صدر عن علي سعيدي، ممثل علي خامنئي، عندما نجحت الهجمة التي شنها جيش فضاء إيران السيبراني على موقع صوت أميركا *VOA* في شهر فبراير عام 2011 حيث أعلن فيه صراحة أن هذه الهجمة تعد برهاناً ساطعاً على السطوة السيبرانية للحرس الثوري الإيراني، وقدرته على بلوغ أهدافه في أي رقعة من فضاء الفيض السيبراني للولايات المتحدة (*Mansharof,2013*).

4 . 4 . 2 . فصائل ميليشيا الباسيج السيبرانية:

تنظيمياً، تستقر منظمة الباسيج في الطبقة التي تلي مؤسسة الحرس الثوري الإيراني، وتدين بالولاء التام لخطاطتها، وتعكف على تنفيذ برامجها في فضاء إيران السيبراني، إلا أنه قد أوكلت لفصائل ميلشياتها السيبرانية مهمة المنافحة عن المجال الثقافي والعقدي للثورة الإسلامية بإيران،. مع وجود تداخل في المهام، شأن الأدوار التي تمارسها مؤسسات

---

[172] . في تصريح لجريدة همشري اليومية، التي تصدر في إيران، ذهب القيادي في الحرس الثوري الإيراني، جيربادي، أن جيش فضاء إيران السيبراني ليس سوى منتدى أو قاعدة عريضة وجامعة للناشطين السيبرانيين وقراصنة المعلومات الإيرانيين الذين يدافعون عن بلادهم، وثورتهم الإسلامية ضد الهجمات التي يمارسها أعداء إيران، وبهيكلة مؤسسية مفتوحة بعيداً عن أي نمط من أنماط الهياكل المؤسسية . التقليدية.

إيران المختلفة، مع قوات كربلاء السيبرانية التي تلتزم بجزء من هذا المحور أيضاً أثناء حضورها في فضاء إيران السيبراني.

وينضوي تحت جناحي هذه المنظمة كل من مجلس الباسيج السيبراني، وشرطة فضاء إيران السيبراني *FATA* واللذان يتكامل عملهما من خلال ترسيخ فضاء وطني آمن تسهر قوات الشرطة السيبرانية على حماية امنه من تجاوزات قراصنة المعلومات المناوئين للنظام، مع كف جرائم المعلومات بمختلف أشكالها، وفي ظل سنّ تشريعات وقوانين تحكم قبضة هذه المنظمة على كافة أشكال الممارسات التي قد تتعارض مع منظومة ثقافة النظام، والتي تبرز، هنا، وهناك في فضاء يزدحم بمستخدمين، متعددي المشارب والتوجهات، ولديهم مهارات معلوماتية واتصالية لا يستهان بها.

وقد حظيت الباسيج بحصار اقتصادي وتقني من الإدارة الأمريكية بسبب متابعاتها وإجراءاتها الغاشمة ضد المعارضة الإيرانية خلال حملة الانتخابات الرئاسية عام 2009.

وأسهم نجاحها في إخماد صوت المعارضة، وتكميم خطابها الذي حاول أن التسلل بتغريدات رقمية مناهضة عبر موقع التغريد السيبراني *Twitter*، ونشرها لمقاطع فيديوية تعلن عن تجاوزات النظام في مواجهة المعارضة في شوارع طهران وأزقتها عبر موقع *YouTube* في جعل النظام الإيراني يوليها المزيد من الدعم، فأوكل إليها مهمة مواجهة تيار الهجمات اللينة التي يوجهها الغرب نحو فضاء الانترنيت الإيراني، ومحيطه المعرفي الذي حرص النظام على شحنه بتفاصيل خطاطة الثورة الإسلامية السياسية والعقدية.

وقد هرعت مؤسسة الباسيج الى تشكيل ميليشيا رقمية من المتطوعين لشن هجمات رقمية على مواقع الويب، وكيانات رقمية لجهات معادية أسوة بما قام به الحرس الثوري الإيراني. وقد اعترف الرئيس التنفيذي لميليشيا الباسيج، علي فضلي، في لقاء معه بشهر مارس 2011 أن هناك مجموعة منتخبة من قراصنة المعلومات الإيرانيين الذين تطوعوا للعمل مع مؤسسته في شنّ هجمات على مواقع ويب جهات معادية لإيران (*Kokhreidze,2015*).

وبدأ قراصنة المعلومات المحليين بالتوافد على منظمة الباسيج للالتحاق بصفوف فصائله السيبرانية التي باشرت عملها مع مجلس الفضاء السيبراني بالمنظمة ذاتها منذ بواكير عام 2010، ووفرت لهم برامج تدريبية للارتقاء بمهاراتهم وقدراتهم على الدفاع عن مواقع الويب وتجاوز آثار حضور الفجوات السيبرانية، فبلغ عديد الملتحقين بالدورات التدريبية 1500 قرصان رقمي، في شهر نوفمبر من العام ذاته (*Mansharof,2013*).

وتألفت تشكيلة هذه الميليشيا السيبرانية من متطوعين من أساتذة الجامعات، وطلبة الجامعات من التخصصات العلمية، وطلبة من الحوزات العلمية، وعناصر نسوية، لا يقتصر عملهم على شن هجمات معلوماتية على أهداف خصوم النظام الإيراني، بل يعكفون أيضاً على بث الدعاية الإعلامية لدعم خطاطة الثورة الإسلامية في في فضاء إيران السيبراني وفضاء الانترنيت العولمي. بالمقابل تقوم مؤسسة الباسيج بمنح أعضاء هذه المجموعة مبالغ رمزية لدعم أنشطتهم (*Kokhreidze,2015*)[173].

في البداية، لم تمتلك الفصائل السيبرانية في منظمة الباسيج خبرات عميقة في تقنية المعلومات والاتصالات وأنشطة القرصنة السيبرانية، فاقتصرت أنشطة أفرادها على شن هجمات بدائية على مواقع المعارضة الإيرانية، وكيانات أخرى لا تمتلك أهمية استراتيجية.

---

[173] . تمنح الباسيج أعضاء هذه الميليشيا حوالي 60 دولار عن كل منشور في مدونتهم، بينما تصل المنحة الى 1000 دولار لكل من ينشئ مدونة تحوي خطاباً يدعم خطاطة النظام في فضاء الانترنيت الإيراني.

بيد أن عملية إعادة تنظيم وحدات الحرس الثوري الإيراني، وامتداد تأثيرها الى جناح الباسيج لتطوير القدرات السيبرانية والتهيؤ للولوج الى مجال المجالدة السيبرانية نالت فصائل الباسيج السيبرانية اهتماماً أكبر، وبدأت كوادرها بالتحول من كوادر تمتلك مهارات وخبرات متواضعة (بالمقارنة مع جيش فضاء إيران السيبراني) تعينها بالكاد الى اختراق بعض المواقع، وخدمات البريد الالكتروني، الى كوادر اكثر تطوراً بعد أن بلغتها آثار التخصيصات الكبيرة التي خصصتها الإدارة الحكومية لتطوير آلة الحروب السيبرانية، والارتقاء بخبرات مواردها البشرية.

أما على صعيد بنيتها المؤسسية، فقد توسعت البنية التحتية للمعلومات والاتصالات لمنظمة الباسيج، بحيث أضحت قادرة على استضافة مواقع وإدارة البنى التحتية للمعلومات الخاصة بالوحدات الملحقة بمؤسسة الحرس الثوري الإيراني، في جميع المحافظات الإيرانية، وتوفر على صفحاتها معلومات تخص هذه الوحدات وأنشطتها، وتقدم خدمات متنوعة لمنتسبيها (*HP,2014,a*).

وبالوقت ذاته تكاثر عديد الملتحقين بفصائل ميلشياته السيبرانية[174]، مع تعمّق خبراتهم، وتنامي قدراتهم بحيث أن الفصائل السيبرانية الملتحقة بهذه الميليشيات، والتي تألفت من أساتذة، وطلبة مؤسسات أكاديمية، وطلبة من الحوزات العلمية، تدعمها فصائل نسوية من قوات الباسيج قد باشرت بشنّ سلسلة من الهجمات السيبرانية على مواقع أعداء الأمة الإيرانية. ذكر ذلك علي فاضلي، نائب القائد العام لمؤسسة الباسيج، في تصريح له لوسائل الاعلام الإيراني بشهر آذار عام 2013، وذهب الى أن الحروب التي تندلع في الفضاء السيبراني لن يحالفها النجاح ما لم تتكاتف فيها عمليات الدفاع عن المواقع الإيرانية، على التوازي مع شن هجمات على مواقع الخصم بقصد إضعاف آلته السيبرانية، وكفّه عن ممارسة الهجمات المتكررة على مواقع ويب الثورة الإسلامية[175] (*Mansharof,2013*).

بالمقابل، صاحب إنشاء مجلس الفضاء السيبراني في منظمة الباسيج، طفرة نوعية في الإمكانيات التي بدأت بالنمو تدريجياً لدى فصائل هذه المنظمة، ولم تمر سوى مدة يسيرة حتى أوكلت إليها مهمة إدارة عمليات الحرب اللينة التي مارسها خصوم إيران بكثافة لإحداث خلل أو فجوات داخل منظومة قيم الثورة الإسلامية. فباشرت فصائل منظمة الباسيج مهامها وبدأت بسد الثغرات والفجوات التي يمكن أن يستثمرها خصوم إيران في تسريب خطابهم السياسي والثقافي الى الفضاء السيبراني في إيران، وهرعت الى نشر خطاب الثورة الإسلامية، وخطاطتها العقدية في فضاء الانترنيت العولمي وفق استراتيجية دعائية دعمتها الحكومة بشتى أنواع الدعم المالي والمعنوي.

وقد وسعت الباسيج من مجال نشاط ميليشيتها السيبرانية، فبدأت ببسط سلطانها على فضاء الفيض السيبراني الإيراني، وبدأت تمارس عمليات التجسس على الناشطين الإيرانيين المعارضين للنظام، مع السعي الى جمع بيانات استخبارية تدعم السلطات الأمنية لإيقاعهم في قبضة المؤسسات الأمنية، أو بيد المؤسسات القضائية بالبلاد[176].

وإضافة الى كل هذا نكاد نعثر على تصريحات متناقضة أطلقها السياسيون الإيرانيون، هنا او هناك عن تشكيلات قد تتداخل مسمياتها مع تشكيلات أخرى قائمة، أو وهمية، فمن هذه التصريحات ما أعلنه غلام ميرزا جليلي، رئيس منظمة الدفاع المدني في شهر مارس من عام 2010 أن المركز الرئيسي لحروب المعلومات بالدولة الإسلامية سوف يبصر

---

[174] . هرعت مؤسسة الباسيج، في بداية عام 2011، الى الإعلان عن خططها المستقبلية لتجنيد قراصنة المعلومات من مجتمع المعلومات الإيراني للمساهمة الفاعلة في عمليات الحرب اللينة (*HP,2014,a*).

[175] . ذكر قائد فصائل الحرس الثوري الإيراني في طهران، أن عام 2010 شهد نجاح الباسيج في تدريب أكثر من 15,000 عضو متدرب من أعضاء المنظمة على ممارسة حرفة التدوين وأنشطة حروب المعلومات بمختلف أشكالها. بيد أن قائد فصائل مدينة قم أكّد تدريب 2000 عضو من الباسيج على ممارسة القرصنة السيبرانية ومباشرة الهجمات السيبرانية على مواقع خصوم الثورة داخل فضاء إيران السيبراني، وخارجه (*HP,2014,a*).

[176] . في شهر مارس من عام 2011 ذكر أحد القادة الكبار في مؤسسة الباسيج أن جيش فضاء إيران السيبراني يمارس مهامه بوصفه أحد تشكيلات الباسيج، دون أن يفصح عن هوية هذا الجيش (*SenseCy,2014*).

النور في وقت قريب ووجه دعوة الى قراصنة المعلومات الذين يدينون بالولاء للثورة الإسلامية للتعاون مع المركز الجديد ودعمه بخبراتهم لتعزيز قدراته (*IHRO,2014*).

5. احتضان الوكلاء السيبرانيين والبؤر السيبرانية *Iran Cyber Proxies*:

لم تكتفي الإدارة الحكومية الإيرانية بتجنيد جلّ مؤسساتها، العسكرية والأمنية والمدنية، وشريحة واسعة من المواطنين الذين يمتلكون معرفة جيدة في القرصنة السيبرانية، وسبر مواطن الخلل في شبكات المعلومات للعمل معها وتوفير الدعم الكافي لإنجاح استراتيجيتها بشقيها الدفاعي والهجومي، ولكنها لجأت الى تجنيد قطعات رقمية، من خارج حدود البلاد، عن طريق تفويض وكلاء رقميين *Cyber Proxies* للتنسيق المباشر والعمل مع قواتها السيبرانية بتنفيذ مهام محددة ضمن الفضاء الافتراضي للدول المعادية للنظام الإيراني.

وبذلك بسطت مؤسسة الحرس الثوري الإيراني هيمنتها ، وأضحت تسيطر على إدارة مجموعة كبيرة ومتنوعة من وحدات وفصائل حروب المعلومات التي توكل إليها مهام خاص تتوافق مع السياسات العسكرية الأمنية الخاصة بخطاطة هذه المؤسسة الواسعة، يضاف الى ذلك وحدات العمليات المشتركة لمخابرات الاتصالات *Signals Intelligence (SIGINT)*، وفصائل ميليشيات كربلاء للقوى الثقافية في الفضاء السيبراني *Karbala Mazandaran Cyber Culture Forces* والتي تلتحق بها مجاميع أخرى، مثل جيش فضاء السيبراني بتركيبته ومعماريته التنظيمية الفريدة، وفصائل جيش سورية الالكتروني *SEA*، وفصائل وميلشيات رقمية أخرى تتكامل في تشكيل كيان فسيفسائي للدفاع والردع السيبراني[177] لا نكاد نعثر على شبيه له في المنطقة، أو في الفضاء السيبراني العولمي (*HP,2014,a*).

ولضمان بلوغ مستوى متقدم على صعيد السلطان السيبراني، خصصت الحكومة الإيرانية مبلغ مليار دولار لتشكيل وتطوير أفراد وعتاد فصائل جيشها السيبراني الذي تألفت موارده من صفوة النخبة الإيرانية من كوادر المؤسسات الحكومية، وإدارات والقراصنة المتميزين بالشركات الأمنية، وجحافل من المتطوعين الشباب الذين نذروا أنفسهم لشن الهجمات وممارسة عمليات التنقير عن الفجوات السيبرانية تحت راية، وبتوجيه مباشر من قيادة الحرس الثوري الإيراني (*HP,2014*).

ولم تقتصر عملية توظيف هذا المبلغ الكبير لتطوير الآلة السيبرانية بالبلاد، وبناء القدرات المحلية، وإنما توسعت باتجاه توفير الدعم المالي واللوجستي لمجاميع قرصنة وميليشيات رقمية تستوطن خارج الحدود الجغرافية للبلاد، وفي بلدان عربية، مثل: سورية، ولبنان، واليمن، وبلدان أخرى في قارة أمريكا الجنوبية، وبلدان أوربية، مجتمعين تحت راية واحدة تلتزم قياداتها وأفرادها بولاء مطلق لثقافة الثورة الإسلامية، ويأتمرون بأوامر المرشد الأعلى للثورة الإسلامية.

بصورة عامة، يلاحظ وجود تطابق في خارطة التطورات الحاصلة في قدرات مجاميع قراصنة المعلومات الملتحقة مع البؤر السيبرانية التي تحتضنها إيران، مع تلك التي مرّت بها القدرات السيبرانية لمؤسسات الدفاع والردع السيبرانية ـ الإيرانية.

وباستثناء الفصائل السيبرانية لحزب الله اللبناني، وحركة حماس في غزة، واللتان تمتد جذور خبرتهما في ممارسة عمليات الدفاع والردع السيبراني الى العقد الأخير من القرن العشرين فإن ولادة بقية الفصائل والوكلاء السيبرانيين قد

---

[177] . رغم أن تصريحات جل المسؤولين الإيرانيين، ومن مختلف المؤسسات والهيئات التي ينتمون لها تؤكد أن ما تقوم به هذه مؤسسة الحرس الثوري الإيراني وغيرها من الفصائل لا تعدو عن كونها مهمة دفاعية عن حياض فضاء إيران السيبراني، إلا أن البينات المتوفرة لم تعد تسعف الإيرانيين في إخفاء ممارسات الردع السيبرانية التي حرصوا عليها، وعمدوا الى تكثيفها في الفضاء السيبراني، وبالخصوص بعد هجمات الفايروس الخبيث *Stuxnet* على وحدات تخصيب اليورانيوم عام 2009.

ارتبطت بنشوب الصراعات في بلدانهم (الجيش السوري السيبراني عام 2011، وجيش فضاء اليمن السيبراني 2012)، والتي تعود الى العقد الأول من الألفية الجديدة.

وقد نجحت مؤسسة الحرس الثوري الإيراني في إدارة وتنسيق أنشطة الدفاع والردع السيبراني على مستوى عولمي، وبواسطة مجموعة من الوكلاء السيبرانيين مثل: جيش حزب الله السيبراني، وجيش سوريا الالكتروني، ومقاتلي القسام بالفضاء السيبراني، والفصائل المجهولة للجهاد الافتراضي، وفصائل الباسيج السيبرانية، وبتنسيق مباشر مع مجاميع القرصنة المحليين مثل فريق مجموعة *Ashiyane*، ومجموعة *Shabgard*، ومجموعة *Parastoo* (*IFR,2013*) وأصبحت تهيمن على قوى رقمية ذات سلطان رقمي كبير، ويمتد نشاطها على مساحة واسعة من الفضاء السيبراني العولمي[178].

5 . 1 . الفصائل السيبرانية لحزب الله اللبناني:

أسهمت مرابطة فصائل حزب الله على خط المواجهة مع جيش الكيان الصهيوني، وتطوّر الآلة السيبرانية وادواتها لدى خصمه العنيد على دفع قيادة الحزب نحو تطوير قدراته السيبرانية والاتصالية بحيث تفوقت عدّتها وعتادها على الكثير من نظم المعلومات الموجودة في الجوار (الرزو، 2008).

في البداية، اقتصرت الأنشطة السيبرانية التي مارستها الفصائل السيبرانية في حزب الله على ممارسة الحرب الإعلامية والنفسية ضد الكيان الصهيوني مع الحرص على نشر الخطاب السياسي والعقدي للحزب والذين يدين بالولاء للخطاطة العقدية لولاية الفقيه التي احتضنها النظام الايراني(*Cohen-Almagor,2012*).

5 . 1 . 1 . الاستراتيجية السيبرانية لحزب الله :

أثبت حزب الله في أكثر من واقعة سعيه الدائم والمحموم لضمان حصوله على ميزة ترسّخ تفوقه في صراعه الدائم مع الكيان الصهيوني. وقد انتبهت قيادات هذا الحزب الى الدور الكبير الذي باتت تلعبه تقنيات المعلومات والاتصالات وادواتها في مجتمع المعلومات المعاصر، وحجم تأثيرها البالغ على تسيير دفة أنشطة المواجهة مع الخصم على ساحة الفضاء المتخيّل، فسعت الى إنشاء بنية تحتية من موارد المعلومات والاتصالات مع تهيئة وتدريب قوى بشرية قادرة على إدارة دفتها في ميدان المواجهة السيبرانية المستمرة مع الكيان الصهيوني[179].

بصورة عامة حدّدت إدارة نظام المعلومات في حزب الله سياسة حضورها وطبيعة ممارساتها المعلنة في فضاء الانترنيت بما يأتي (*M.I.T.I.C,2013*):

- ✓ السعي الى تضخيم الدور الذي يمارسه أمين الحزب حسن نصر الله في ترسيخ الدور الذي يمارسه الحزب بالمنافحة عن الجنوب اللبناني ومدافعة العدوان الصهيوني، وذكر بطولات شهداء الحزب أثناء دفاعهم عن الأرض اللبنانية، ودعوة الآخرين للاقتداء بسيرتهم.

[178] . في إحدى تصريحات القائد الأعلى للحرس الثوري الإيراني، محمد علي جعفري، بشهر شباط من عام 2011، أكد أن إيران تتلقى دعماً سخيّاً من مجاميع لقراصنة المعلومات، تقيم في دول خارج حدود إيران، تجمعها قواسم مشتركة في مناهضة دول غربية، أو مؤسسات تهيمن على آلة الاقتصاد العولمي، بحيث تمارس عملية تنسيق الهجمات بين الطرفين بكفاءة عالية، وستشكل هذه المجاميع قوات دعم إضافية لقوة الردع السيبرانية في إيران في حالة نشوب نزاع رقمي مع الدول التي تعادي الثورة الإسلامية (بحسب تصريحه) (*Mansharof,2013*).

[179] . ولشدّ الشباب وجذبهم الى ممارسة فعل المقاومة تجاه العدو الصهيوني، ابتكر الحزب لعبة رقمية أطلق عليها اسم "القوة الخاصة" وأضحت في متناول مستخدمي الحاسب في لبنان وسورية مع اطلالة عام 2003. تعرض اللعبة مشاهد واقعية من المواجهات بين فصائل حزب الله وقوات الكيان الصهيوني، مع صور التقطت من أرض الواقع. وقد تضمنت اللعبة خياراً للتدريب على ممارسة الهجمات حيث يستطيع ممارس اللعبة اختيار السلاح الذي يروم استخدامه، والأهداف التي ينوي مهاجمتها، أو إحدى الشخصيات السياسية أو العسكرية التي يريد اغتيالها. وبتقدم اللاعب وانجازه للمهام القتالية يحصل على المزيد من النقاط التي تتكلل بحضور احتفالية متخيلة مع قائد الحزب نصر الله! (*M.I.T.I.C,2013*).

- ✓ بيان طبيعة الدور الذي يمارسه الحزب في مقاومة المحتل من خلال ممارسة مختلف أنماط الحروب النفسية على الكيان الصهيوني، وتوظيف آليات الدعاية الإعلامية السيبرانية بأشكالها المختلفة.
- ✓ بسط الدعوة الى مبادئ حزب الله عبر وسائط الانترنيت وبيان الثوابت التي تلتزم بها قيادته، وتأكيد التحاقه بركب الثورة الإسلامية في إيران، وولائه المطلق للمرشد الأعلى علي خامنئي.
- ✓ نشر خطاطة الثورة الإسلامية في إيران، ودرء الشبهات عن مبدأ ولاية الفقيه الذي جاء به الامام الخميني، والدعوة للوقوف بقوة ضد الولايات المتحدة وحلفائها بالمنطقة لدرء التهديدات والأخطار التي قد تمسّ إيران فتصل آثارها الى حزب الله الذي يوالي النظام الإيراني ويسير على هدى توجيهات المرشد الأعلى للثورة.
- ✓ دعم فصائل المقاومة الفلسطينية في مواجهتها للعدوان الصهيوني، وفسح المجال أمام استخدام مواقعه لنشر المادة التي تعبر عن الانتهاكات الصهيونية، ونضال الشعب الفلسطيني في دفع العدوان ومقاومة الاحتلال.

وقد استمر اقبال حزب الله على الفضاء السيبراني وتوظيفه، بوصفه فضاء مفتوحاً لمباشرة حرب نفسية وإعلامية ضد الكيان الصهيوني، مع استثمار القدرات المتاحة في فضائه المفتوح لنشر خطابه السياسي والعقدي، وبث خطاب المقاومة على مجال واسع[180].

أسهمت المواجهات العنيفة خلال الحرب اللبنانية الثانية والتي نشبت عام 2006 الى توسيع رقعة اهتمام حزب الله بحضوره السيبراني في فضاء الفيض السيبراني، بعد أن ثبت لدى قياداته نجاعتها في الحرب غير المعلنة مع الكيان الصهيوني (الرزو،2008).

بيد أن هذه السياسة قد شهدت انعطافاً نحو ممارسة سجال رقمي لتثبيط وخلخلة عمل مواقع الويب لخصوم حزب الله، مع بدايات العقد الأول من الألفية السابقة، وبعد أن تكاثرت هجمات الفصائل السيبرانية للجيش الإسرائيلي، وقراصنة إسرائيليين متطوعين على مواقع الحزب وشبكاته الإعلامية، فتوجهت الإدارة السيبرانية في الحزب نحو تطوير قدراتها الدفاعية مع البدء بتطوير قدراتها الهجومية للبدء بمرحلة تحوّل جديدة نحو ترسيخ قدراتها الدفاعية والهجومية السيبرانية.

وبمرور الزمن نجحت إدارة حزب الله اللبناني في تنمية وتطوير قدراتها وسلطانها السيبراني لتلبية سياستها في توظيف الأداة الجديدة لمناضلة الكيان الصهيوني، بحيث أضحت محط اهتمام وكالة المخابرات المركزية الأمريكية منذ منتصف عقد التسعينات بالقرن الماضي[181]. ولم تمر سوى بضع سنوات (في عام 2002 بالتحديد)، قامت وكالة المخابرات المركزية بتقديم تقرير الى لجنة الأمن بالكونغرس حددت فيه هوية مجموعة من المنظمات الإرهابية، كان اسم حزب الله مدرجاً في هذه القائمة، مؤكدة أنه يمتلك الرغبة والقصد لتطوير بعض أشكال المهارات السيبرانية التي تمنحها القدرة على ممارسة مجموعة من الهجمات السيبرانية عبر الالفضاء السيبرانيي للانترنيت(*Conway,2003*).

---

[180] . يمكن تلمّس بصمة هذه السياسة السيبرانية من خلال تصريح علي أيوب (المدير المسئول عن إدارة وتشغيل 11 موقع ويب لحزب الله على الانترنيت) وتأكيده أن حزب الله لا يستخدم الانترنيت إلا بوصفها مورداً ثرياً للمعلومات، يمكن استثمارها في الحملات الإعلامية على شبكة المعلومات لترسيخ كفاح الشعب العربي ضد الانتهاكات الصهيونية (الرزو،2008).

[181] . ورد في شهادة المدير السابق لهذه الوكالة *John Deutch* أمام اللجنة الفرعية الدائمة للشئون الحكومية بالكونغرس الأمريكي في منتصف عام 1995 العبارة الآتية : " إن المجاميع الإرهابية الدولية باتت قادرة على تهديد ومهاجمة البنى التحتية للمعلومات للولايات المتحدة، حتى وإن لم يتوفر لديها سوى أدوات معلوماتية بدائية. ونعتقد أن بعض المجاميع التي تمتلك خبرات تدعمها في استخدام الانترنيت وأدوات الاتصال السيبراني في تعزيز قدراتها الاتصالية، مثل منظمة حزب الله قادرة على مباشرة تهديدات معلوماتية على البنية التحتية للمعلومات"(*Deutch,1996*).

5 . 1 . 2 . مراتب الحضور السيبراني لحزب الله في الفضاء السيبراني:

وضع حزب الله اللبنة الأولى لحضوره السيبراني في فضاء الانترنيت في بداية عام 1996 على صفحات الموقع الرسمي للحزب *Hizbollah.org* وطرح مادة المحتوى السيبراني للموقع باللغتين العربية والإنجليزية لضمان وصول خطابه الى شريحة عريضة من مستخدمي شبكة الانترنيت (الرزو،2008).

وبعد مدة قصيرة أضيف الى قائمة مواقع الحزب ثلاثة مواقع جديدة هي:

- ✓ موقع المقاومة الإسلامية الذي يعرض بطولات مقاتلي حزب الله وهجماتهم المتوالية على مواقع العدو الصهيوني.
- ✓ موقع تلفزيون المنار الذي يعرض الأخبار، ويحوي على الصفحة الرئيسة لقناة المنار الفضائية الناطقة بلسان قيادة حزب الله.
- ✓ موقع السيد حسن نصر الله الذي يضم الصفحة الرسمية لقائد الحزب السيد حسن نصر الله.

وقد تزايد أعداد مواقع الويب التي سخرها الحزب للإعلان عن خطاطته السياسية والعقدية، ونشر خطابه الإعلامي ضد الكيان الصهيوني حتى بلغ عديدها أكثر من عشرين موقعاً، وتعددت لغاتها حتى أضحت هذه المواقع تحسن النطق بسبع لغات حيّة[182] لضمان بلوغ خطاب الحزب الى طيف واسع من مستخدمي شبكة الانترنيت.

وقد قسم التقرير الصادر عن مركز *Meir Amit* الإسرائيلي (الذي يعنى بتتبع نشاطات حزب الله على أرض الواقع والفضاء المتخيِّل) مراتب حضور حزب الله اللبناني في فضاء الانترنيت الى سبع فئات رئيسة (*M.I.T.I.C,2013*):

- ❖ الفئة الأولى: مواقع إخبارية تعنى بنشر نشاطات الحزب المختلفة وإلقاء الضوء على العمليات التي يقوم بها جند الحزب ضد قطعات الجيش الصهيوني وتجمعاته. ومن هذه المواقع: موقع المقاومة الإسلامية في لبنان، وموقع الإنباء، وموقع دعم المقاومة الإسلامية في لبنان، وموقع الوعد.
- ❖ الفئة الثانية: مواقع حزب الله الإعلامية التي تمارس حضوراً موازياً للنشاط الإعلامي الذي تمارسه الآلة الإعلامية للحزب على مواقع الانترنيت. ومن هذه المواقع: موقع محطة المنار الفضائية، وموقع محطة إذاعة النور، ومواقع صحف الحزب مثل موقع الانتقاد.
- ❖ الفئة الثالثة: مواقع المؤسسات الاجتماعية لحزب الله والتي تقوم بنشر أنشطة الحزب في توفير الدعم لمختلف قطاعات الحياة الاجتماعية للمجتمع الشيعي في لبنان، بالإضافة الى الدفع الذي توفره للمقاومة وأفرادها. ومن هذه المواقع: موقع مؤسسة الشهيد، وموقع الجهاد البناء، وموقع موسوعة الجرحى، وموقع الهيئة الصحية الإسلامية، وموقع كشافات الامام المهدي، وموقع جمعية مرشدات المهدي، وموقع جمعية الإمداد، وموقع المعهد الإسلامي للدراسات، وموقع جمعية المعارف، وموقع جمعية أصدقاء البيئة، ومواقع مناهضة للكيان الصهيوني، منها موقع دار الهادي، ومواقع نشر فكر الامام الخميني، منها مواقع المراكز الثقافية التي ترعى أنشطة جمعية مراكز الخميني الثقافية بعموم لبنان، وموقع شبكة الشيعة التي تزخر بمعلومات عن الخطاب العقدي الشيعي.
- ❖ الفئة الرابعة: مواقع حزب الله المحلية التي تقيم في الفضاء السيبراني اللبناني، والتي يستوطن نشاطها السيبراني في كل من قرى: بنت جبيل، والطيبة، والجبشيت.

---

[182] . تنطق مواقع ويب الحزب باللغة العربية، والانجليزية، والفارسية، والفرنسية، والعبرية، والاسبانية، والأذربيجانية.

- ❖ الفئة الخامسة: مواقع خصصت لنشر مآثر القيادات السابقة والحالية لحزب الله، ومنها موقع الصمود، ومواقع تمتدح رئيس الحزب حسن نصر الله.
- ❖ الفئة السادسة: منتديات رقمية مرتبطة بخطاطة حزب الله، منها: موقع قاوم.
- ❖ الفئة السابعة: مواقع محلية للتواصل الاجتماعي والمشاركة بالمحتوى السيبراني (المرئي، والسمعي، والمدوّن) لرفع وتداول المقاطع الفيديوية التي توثق نشاط الحزب على موقع *YouTube*، ونشر التغريدات السيبرانية التي تنافح عن الحزب في فضاء التغريد السيبراني *Twitter*، أو إطلاق المنشورات والتعليقات على صفحات شبكة التواصل الاجتماعي *Facebook*.
- ❖ وأظهرت أكثر من دراسة أن الحضور السيبراني للحزب يستضاف في شركات مضيفة بالولايات المتحدة وكندا تقدم له الدعم التقني والسيبراني (64% من المواقع تستضاف لدى شركات أمريكية، 27 % لدى شركات لبنانية، بينما لا تتجاوز نسبة المواقع التي تستضاف لدى شركات لبنانية محلية على 9%)، بينما هناك موقعين فقط من مواقع حزب الله يستضافان خارج حدود مجهزات الخدمة الأمريكية، أحدهما يستقر لدى مجهز خدمة بإيران، والثاني لدى مجهز خدمة ببريطانيا (الرزو،2008).

5 . 1 . 3 . مطالع التحالف السيبراني بين حزب الله وإيران وآثاره:

لم يقتصر طموح النظام الإيراني على توسيع نطاق هيمنته في المنطقة على المشاركة المباشرة وغير المباشرة في النزاع الدائم بين حزب الله والكيان الصهيوني على ساحة النزاع بالشرق الأوسط، وحاول فتح جبهة من نمط آخر للمواجهة الجديدة مع الكيان الصهيوني في فضاء الفيض السيبراني، من خلال وكيل رقمي يدين بالولاء لخطاطته العقدية والسياسية، ويكون اهلاً للحصول على قدرات وسطوة رقمية بالمنطقة، فوقع اختياره على حزب الله، حليفه الأول في منطقة الشرق الأوسط. وقد قبل حزب الله بممارسة د ور الوكيل السيبراني لإيران في فضاء المنازعة المتخيّل مع الكيان الصهيوني، العدو المشترك، ليحقق غايتين، الأولى: تعزيز الشراكة مع النظام الإيراني وتسديد جزء بسيط من الفضل الذي يستحق كل عرفان للدعم غير المسبوق في دعم الحزب مالياً، وعسكرياً ولوجستياً على صعيد النزاع المحتدم مع الكيان الصهيوني، والثانية: تعميق قدرات أفراد الحزب في مجال فضاء الفيض السيبراني الذي قد بلغت كوادر الكيان الصهيوني مراحل متقدمة على المستوى العولمي، مما يوفر للحزب حصانة تجاه التهديدات والهجمات التي تمارسها فصائل الجيش الإسرائيلي ضد الحضور السيبراني للحزب في فضاء الانترنيت.

فبدأ الطرفان بالتعاون على إنشاء منظمة جديدة، ترتبط بالمؤسسة السيبرانية ـ الإيرانية، بالغة التعقيد، والتي تمتلك أكثر من وكيل لبسط سلطانها السيبراني في المنطقة. وكان ثمرة هذا التعاون والتنسيق المشترك بين الطرفين، ولادة مؤسسة فضاء الفيض السيبراني لحزب الله *Cyber Hezbollah* التي تسارعت مراحل نموها بعيد المواجهة الشرسة للحزب مع الكيان الصهيوني عام 2006، وبدأت تحقق قفزات نوعية على مستوى التهديدات والهجمات التي باشرت بممارستها ضد العدو المشترك في الفضاء المتخيّل، لتضيف الى معادلة توازن القوى متغيراً جديداً يعزز موقف الحزب ويمنح إيران فرصة إضافية للتغلغل في نسيج النزاع المحتدم في المنطقة، بالإضافة الى منح إيران لتحقيق استراتيجيتها وغاياتها دون أن تترك بصمات مباشرة يمكن أن تثبت تورطها فيما يدور من أحداث بمنطقة النزاع (*Cilluffo,et.,al.,2012*).

باشرت المؤسسة السيبرانية الجديدة في حزب الله عملها في شهر يونيو من عام 2011، بعد أن حددت لها مجموعة من المهام والأهداف التي تضمنت (*Cilluffo,2012*): تدريب وبناء القدرات لنخبة من قراصنة المعلومات المنتمين

للحزب على ممارسة سلسلة من عمليات القرصنة على مواقع إسرائيلية، وتطوير آلة وأدوات الدفاع والهجوم السيبراني، البدء بالخطوة الأولى على صعيد بناء القدرات الهجومية والولوج في ميدان الحروب السيبرانية.

وقد آتى هذا التحالف ثماره بصورة سريعة، فتعزز سلطان حزب الله في فضاء الفيض السيبراني وبات يمتلك قدرات مميزة على صعيد المواجهات المستمرة مع الكيان الصهيوني، كما أسهم بالوقت ذاته في تعميق هيمنة النظام الإيراني على أجزاء غير منظورة من ساحة الصراع مع الدول والأنظمة التي تناهضه بالمنطقة، وتوفير بيانات ثمينة مضافة الى الحصيلة التي تمتلكها مؤسساته السيبرانية العسكرية والمخابراتية.

لقد أضاف التحالف الجديد، الى القدرات السيبرانية لحزب الله، فرصة ممارسة نمط جديد من المساجلة السيبرانية داخل حدود الفضاء السيبراني، فبعد أن اقتصرت المساجلة السيبرانية على حروب إعلامية، أو خلخلة أداء مواقع الخصم، أو طمر خطابات معادية في المحتوى السيبراني لصفحات الويب (*Osipova,2011*)، وفر التحالف فرصة مباشرة تهديدات وهجمات رقمية لتهديد أمن الفضاء السيبراني الإسرائيلي، ودرء المخاطر المحتملة عن مواقع حزب الله المستوطنة في فضاء الانترنيت.

ولم تمر سوى مدة يسيرة حتى بدأت طلائع مجاميع قراصنة المعلومات التي تدين بالولاء الى حزب الله بالتناسل في فضاء المواجهة وممارسة هجماتها المتتالية على مواقع الكيان الصهيوني، ومواقع المعارضة الإيرانية بالوقت ذاته. ومن هذه المجاميع فريق جهاد فضاء الفيض السيبراني ـ المجهول *The Unknown Cyber Jihad* الذي فرض بصمة حضوره في فضاء المنازعة السيبرانية بعيد ولادته في عام 2013 (*Siboni&Kronenfeld,2014*).

5 . 2 . الجيش السوري الإلكتروني (*SEA*) *Syrian Electronic Army*:

تتألف فصائل الجيش السوري الالكتروني[183] من مجاميع من طلبة الجامعات السورية ومجاميع من قراصنة المعلومات المتحالفين معهم ممن ينتمون الى تنظيمات حزب البعث ويدينون بالولاء لخطاطته السياسية، ويلتزمون بالدفاع عن نظام بشار الأسد وتوسيع نطاق الدعاية لنظامه[184].

ويعد الجيش السوري الالكتروني من أهم الحلفاء والوكلاء السيبرانيين لبرنامج الدفاع والردع السيبراني للنظام الإيراني، حيث ارتبطت بداية تشكيل هذه القوة السيبرانية بمجموعة من قراصنة المعلومات السوريين الذين حاولوا الدفاع عن نظام بشار الأسد من خلال سلسلة هجمات معلوماتية، وجهت مساراتها نحو مواقع ويب لجهات مناوئة لخطاطته السياسية، منذ بدايات عام 2011.

ويشكل كل من قراصنة المعلومات السوريين حاتم ديب (يطلق على نفسه اسم *Th3Pr0*)، وعلي فرحه، وثالث يطلق على نفسه اسم *Th3Shad0w* العمود الفقاري لمجاميع القرصنة في الجيش السوري الإلكتروني[185]، بينما يدعي كل من القرصانين الأول والثالث زعامتهما وقيادتهما لجل الأنشطة التي يمارسها أفراد هذا الجيش[186] (*HP,2014*).

---

[183] . وتطلق المجموعة على نفسها، في بعض الأحيان، اسم الجنود السوريين الإلكترونيين (*Lohlker,2015*).

[184] . أعلن أعضاء هذه المجموعة عن هويتهم، أنهم مجموعة من الشباب السوريين المتحمسين الذين رفعوا عن نفوسهم غبار السلوك السلبي تجاه الهجمات وعمليات تضليل الحقائق التي تمارس لتشويه ما يحصل على أرض الواقع بعيد أحداث الربيع العربي في سورية (*O'Connell,2015*).

[185] . بحسب المعلومات التي حصل عليها الباحث *Brain Krebs* ونشرها في إحدى صفحات مدونته السيبرانية أن حاتم ديب يشغل منصب قائد قسم العلميات الخاصة في الجيش السوري الالكتروني، وأنه يقيم خارج سوريا، في روسيا بالتحديد.

[186] . تشير المعلومات الى أن كل من حاتم ديب وعلي فرحه متقاربان في فتئهم العمرية، وأنهما قدر تخرجا من جامعة *Kalamoom University* (*HP,2014*).

ويتخفى وراء الأركان القيادية الثلاثة لهذا الجيش مجموعة من المتطوعين من قراصنة المعلومات السوريين، والذين بلغ عددهم في بداية عام 2014 بضعة آلاف (بحسب الرواية التي نقلها الباحث *Wilhelmsen* عن إحدى قادة هذه المجموعة *Th3Pr0*) وهو رقم مبالغ به الى حد كبير(*Wilhelmsen,2014*).

تستوطن الفصائل الافتراضية للجيش السوري الالكتروني في الفضاء السيبراني السوري، والذي عمدت الى توظيفه كقاعدة لانطلاق التهديدات والهجمات التي تمارسها ضد الخصوم والمعارضين.

وأسهمت خطاطته الداعمة لنظام الرئيس بشار الأسد، وممارسته لسلسلة من الهجمات التي باتت توجع الكثير من المؤسسات بالولايات المتحدة الأمريكية، ودول أخرى تناصب بالعداوة النظام ذاته، في تعريض حضور هذه المجموعة في فضاء الانترنيت الى المضايقات المتكررة، والتسبب في إغلاق موقعه، وتغيير عنونة الشركات المضيفة لحضوره السيبراني، شأن الكثير من مواقع الكيانات الداعمة للنظام السوري. فبعد أن أقام لأكثر من سنة ضمن مضيف جمعية الحاسب السورية اضطر الى مغادرة مضيفها في عام 2013، ثم وجد له مكاناً في مضيف خدمة يستقر لدى شركة مضيفات في موسكو تدعى *Shorefront Media*، قبل أن يضع رحاله لدى شركة لمضيفات الخدمة بدمشق (*Lohlker,2015*).

اتسمت هجمات أفراد هذه المجموعة، خلال السنة الأولى، بكونها هجمات بدائية حاولت أن تستثمر إمكانياتها ومهاراتها المتواضعة في قطاع القرصنة السيبرانية في الكشف عن الثغرات السيبرانية في مواقع ويب لا تمتلك مستوى رصين من الحصانة الأمنية تعود الى مواقع إخبارية وأخرى تعود الى مواقع أخبار، وبالغوا في إغراقها بهجمات رفض الخدمة وملفات البريد المزعج *Spam* لضمان إنجاح هجماتهم بالآليات البدائية التي تتناسب مع مهاراتهم المتواضعة (*Kagan&Stiansen,2015*).

بيد أن نزعة الهجمات التي مارسها أفراد هذا الجيش خلال عام 2012 اتسمت بتوظيف تقنيات وآليات قرصنة اشد تعقيداً، مما وسّع نطاق الهجمات باتجاه مواقع أكثر حصانة، فنجح في اختراق مواقع حكومية، ومواقع مصارف وشركات أثرت بشكل ملموس على البيئة الاقتصادية للبلدان التي تقيم في فضائها هذه المواقع.

أما في عامي 2013 و2014 فقد اتسمت أنشطة الجيش السوري السيبراني بالتوجه نحو انتاج طيف واسع من البرمجيات الخبيثة والفايروسات، وأجيال من حصان طروادة *Trojan Horse* لتوسيع نطاق التهديدات، وضمان حصول تأثيرات موجعة في الموقع التي تستهدف بهجمات فصائله السيبرانية. وقد أسهم هذا التطور في تمكين فصائل هذا الجيش بشن أنماط جديدة من الهجمات طالت مضيفات الخدمة، وشركات الاتصالات عبر شبكة الانترنيت مثل: *Viber, Tango & True Caller* واستراق كم هائل من بيانات المستخدمين التي استودعت في قواعد بياناتها فشكلت مورداً مهماً للمخابرات السورية لتتبع مسارات شبكة العلاقات الرابطة بين المعارضين للنظام مع توفير فرصة لتحديد هويتهم (*Kagan&Stiansen,2015*).

وشأن مجاميع قراصنة المعلومات في إيران، فقد قام أعضاء الجيش السوري الإلكتروني في عام 2011 بإنشاء مؤسسة أكاديمية ـ افتراضية لتجنيد وتدريب المتطوعين من قراصنة المعلومات السوريين، ممن يرومون الالتحاق بفصائل هذا الجيش، وأطلقوا عليها اسم " مدرسة القراصنة السوريين" (*Wilhelmsen,2014*).

وباشرت هذه الأكاديمية الافتراضية بإعطاء دروس تفاعلية حول كيفية ممارسة هجمات رفض الخدمة *DoS*، واختراق الحواسب، ونظم المعلومات، وممارسة عمليات التلصص على شبكات المعلومات المختلفة. وفي الوقت ذاته بدأ الجيش السوري الالكتروني بتوسيع وتطوير دائرة أنشطته فأنشأ موقع ويب لنشر تسريباته من الوثائق والملفات تعود الى حكومات تناهض النظام السوري، وكان من هذه الوثائق ملفات نجح قرصنته بالظفر بها من مواقع تعود للحكومة

التركية، وأخرى للسعودية، ومجموعة ثالثة تعود الى دولة قطر لإثبات طبيعة الدور الذي تمارسه هذه الدول في تأجيج الحرب الأهلية في البلاد (*INSEA,2013*).

بصورة عامة، تتوزع أنشطة قراصنة المعلومات الملتحقين بالجيش السوري الإلكتروني على ثلاثة محاور رئيسة، يستوطن اثنان منها في بيئة تطبيقات شبكات التواصل الاجتماعي *Facebook & Twitter*، بينما يستثمر الثالث الفضاء الذي يحتضن مواقع الويب لمباشرة مختلف أنماط التهديدات والهجمات السيبرانية (*Wilhelmsen,2014*).

وقد نجحت مجموعة الدراسات الأمنية في مؤسسة *Hewlett Packard* الأمريكية في الكشف عن الكثير من الأدلة والوقائع التي تؤكد على هذا التعاون والتحالف الحميم بين الجهتين. ففي أثناء الهجمات الكبيرة التي قام بها الجيش السوري الإلكتروني عام 2011 تبين أن البرمجيات التي استخدمت في شنّ هذه الهجمات (*Connect Back Backdoor Shell vs 1.0*) هي من صنع القرصان LorD الذي ينتمي الى مجموعة القراصنة الإيرانيين *Sabotage*، كذلك لوحظ مستودع بيانات نظام هذا الجيش يحتوي على شيفرة برمجية تعود الى مجموعة قراصنة المعلومات الإيرانيين *Mormoroth* (*HP,2014,a*).

كما كشفت الكثير من المؤسسات الأمريكية والإسرائيلية، اللثام عن وجود شراكة غير معلنة، وبعيداً عن الفضاء المتخيّل للانترنيت، بين القيادات السياسية والعسكرية السورية والإيرانية، والتي تؤشر الى وجود علاقات مناظرة في الفضاء السيبراني، نذكر منها، البرنامج الاستخباري المشترك بين البلدين *SIGINT* والذي يوفر معلومات مخابراتية ثمينة للبلدين ولحزب الله اللبناني داخل حدود الالفضاء السيبرانيي وخارجه، على حد سواء (*HP,2014*).

ورغم كل هذه الحقائق تستمر قيادة الجيش السوري الإلكتروني في إنكار وجود أية علاقة تربطها بالنظام، وتصرّ على أنها مؤسسة مدنية تندفع بأنشطتها نتيجة للحس الوطني، والحرص على سلامة سورية من آثار العدوان، والحفاظ على أرواح الشعب السوري من الهجمات التي تطالهم، هنا، وهناك[187].

ورغم كل هذه الادعاءات فلا يمكننا القبول بها، وتصديق ادعاء استقلالية هذه المجموعة عن نظام بشار الأسد لأسباب عدة، منها (*Wilhelmsen,2014*):

- ☒ ممارسة هذه المجموعة لأنشطة القرصنة السيبرانية من داخل حدود الفضاء السيبراني السوري دون وجود أية متابعة أو حظر لأي من نشاطاتهم رغم السياسات الصارمة التي يتبناها النظام مع الأنشطة السيبرانية التي يمارسها المستخدمون السوريون عند حضورهم في فضاء شبكة الانترنيت.
- ☒ تسجيل اسم نطاق موقع الجيش السوري الالكتروني (*Syrian-es.com*) لدى جمعية الحاسب السورية منذ الخمس من شهر أيار عام 2011، وهي الجمعية التي أشرف على إنشائها رئيس النظام بشار الأسد قبل أن يتولى زمام السلطة في سورية.
- ☒ وجود ادلة على قيام قريب الأسد رامي مخلوف على دعم أعضاء هذه المجموعة من خلال تسديد أجور شهرية لكل منهم تتراوح بين 500-1000 دولار، بالإضافة الى التنسيق مع مؤسسات تدريبية في لتدريبهم وتطوير مهاراتهم في كل من سورية ودبي وبرعاية مباشرة من قبل النظام الروسي.

[187] . يدّعي أفراد الجيش السوري الالكتروني (في موقعهم *SEA.sy*) استقلاليتهم عن النظام السوري، وأن الهجمات السيبرانية التي يمارسونها ليست سوى رد فعل على النهج الداعم الذي ينتهجه إعلام بعض الدول العربية والدول الغربية لصالح الإرهابيين (بحسب ادعاءاتهم) الذين يمارسون عملية القتل ضد المواطنين السوريين المسالمين، ويمعنون في تدمير كل ما يقع أمامهم من أملاك الحكومة والمواطنين دون مبرر.

- ☒ وجود شواهد عدة على قيام هذه المجموعة بالتنسيق مع أجهزة مخابرات النظام السوري وتزويدها ببيانات عن هوية ومواقع الكثير من رموز المعارضة السورية وأعضائها.
- ☒ امتداح الرئيس السوري لهذا الجيش في أكثر من مناسبة واعتباره فصيلاً مضافاً يدافع عن سورية لأن الجيش السوري يقاتل على الأرض الصلبة، بينما تنافح هذه المجموعة عن سورية في الفضاء السيبراني المتخيَل.

كذلك يوفر النظام السوري دعماً مالياً ولوجستياً لهذا الجيش، والذي عدّه الرئيس السوري بشار الأسد، في إحدى تصريحاته للقنوات الإعلامية، كياناً افتراضياً يقيم في الفضاء السيبراني الوطني، ويمارس دوراً تكميلياً للدور الذي يمارسه الجيش السوري في محاربة أعداء سورية(*HP,2014,a*).

ويتمتع هذا الجيش في الوقت ذاته بدعم تقني ولوجستي من قبل النظام الإيراني، بعد أن شرع النظام الإيراني بتوطيد العلاقة بين قيادة عمليات هذا الجيش وجيش إيران السيبراني ومجاميع القرصنة الملتحقة به، مما منح الطرفين فرصة ثمينة لتوحيد الأهداف، وتنسيق الهجمات على جهات يتفقون على مناهضتهم.

ويمارس هذا الجيش تهديداته وهجماته السيبرانية ضد مواقع المعارضة السورية، ويحرص على تتبع آثار وكشف هوية أفرادها، كما يستهدف كثير من مواقع الويب الحيوية في دول خليجية، وأخرى تعود للولايات المتحدة وحليفاتها (LeClaire,2015). وقد أسهمت الآثار الموجعة لهذه التهديدات والهجمات (على أهداف منتخبة تستوطن فضاء الدول والكيانات المعارضة للنظام السوري، وبلوغها الى أهداف في نسيج المعلومات الغربي) في تصنيف هذه المجموعة ضمن أشد أربع مجاميع القرصنة السيبرانية في عام 2015 (Nightingale,2015).

ويستمر السجال السيبراني بين الجيش السوري السيبراني، وبقية فصائل المعارضة السورية التي تقف على الطرف الآخر منه، سواء على مستوى مجاميع القرصنة الاحترافية مثل الجيش السوري الالكتروني الحر، أو مجاميع تنتمي لفئات سياسية معارضة، أو مواطنين سوريين من داخل البلاد وخارجها، بالإضافة الى الوكلاء السيبرانيين للنظم السياسية المعارضة للنظام ضمن تطبيقات منصات التواصل الاجتماعي، فتتكاثر التبليغات حول وجود مخالفات أو مضامين تتعارض مع المضامين التي تطرحها قيادات الجيش السوري الإلكتروني أو أفراده، مما يعرّض مواقعهم الى الحظر بين الحين والآخر ضمن الحملة التي تتبناها الدول الغربية للضغط على أي نشاط معلوماتي يصب في مصلحة نظام بشار الأسد. لذا نلاحظ ولادة صفحات هنا أو هناك بيد أنها تتعرض للحظر بعد زمن قصير، الأمر الذي حصر ظهور هذه المجموعة من خلال زج شعاراتها في المواقع وصفحات الويب أو مواقع التواصل الاجتماعي التي تفلح في اختراقها بين حين وآخر بعد أن رضيت بأن تقيم في العالم السفلي والمظلم من فضاء الانترنيت بعيداً عن أنظار وملاحقة الخصوم المستديمة.

5 . 3 . الفصائل السيبرانية لكتائب عز الدين قسام:

في البداية، تألفت البنية التحتية لمواقع حركة المقاومة الإسلامية (حماس) على الانترنيت من عشرين موقعاً نطق محتواها السيبراني بثماني لغات (العربية، والإنجليزية، والفرنسية، والروسية، والفارسية، والماليزية، والأوردية، والإندونيسية). وكانت هذه المواقع تدار بواسطة الأستاذ نزار حسين (عضو في حركة حماس ويعمل بوصفه ممثلاً لمكتب معلومات حماس في دمشق، بينما أشرف على تشغيلها مكتب أسامة حمدان (*IDF,2006*).

وسعت الحركة الى توظيف هذه المواقع لنشر خطابها السياسي، وبيان الدور الذي يمارسه الكيان الصهيوني ضد الشعب الفلسطيني، وتوضيح ما يحصل على المشهد الفلسطيني داخل حدود الأرض المغتصبة.

وقد استقرت هذه البنية التحتية للمعلومات الى مضيفات خدمة *Servers* توزعت بين 15 شركة منتشرة في 9 دول داخل حدود الشرق الأوسط وخارجه. فبالنسبة لمواقع حماس يتم استضافتها بواسطة (6 شركات من أوربا الشرقية)، و(3 شركات من دول جنوب شرقي آسيا)، وهناك (4 شركات في أمريكا الشمالية)، وشركتان من دول الشرق الأوسط (*ITIC,2006*).

وقد بذلت الحركة قصارى جهدها لتطوير، وترسيخ حضورها في فضاء مواقع الانترنيت خلال السنوات العشر الأخيرة فعززت خطابها المقاوم بلغات جديدة (مثل اللغة التركية، ولغة الباهاسا، واللغة الإندونيسية)، كما تزايدت أعداد صفحات مواقعها لتتناسب مع التوسع الحاصل في أنشطة الحركة على المستويين السياسي والتنظيمي.

واظهر المسح الميداني لأعداد مواقع ويب حركة حماس على الانترنيت في عام 2015 انها قد قاربت 30 موقعاً، تميزت بحضور رقمي لافت، وبلغات متعددة استوعبت طيفاً واسعاً من مستخدمي شبكة الانترنيت، الذين بدأوا أشد اهتماماً بالمادة المطروحة على صفحاتها.

كما يلاحظ بالوقت ذاته وجود تغير في التوطن الجغرافي للمواقع في مضيفات الانترنيت، فأصبحت المواقع متوزعة على مضيفات بالولايات المتحدة الأمريكية (14 موقعاً)، وأخرى في أوربا (ألمانيا 1، فرنسا 1، أوكرانيا 5، التشيك 3)، و4 مواقع في ماليزية، وموقع في كندا (*WebHostingHero,2015*).

5 . 3 . 1 . الإطار العام لسياسة حركة حماس السيبرانية:

انتهجت حركة حماس نهجاً ثابتاً في ترسيخ حضورها على مواقع الويب، وبما يضمن توسيع دائرة كفاحها الدائم ضد الاحتلال الصهيوني للأراضي الفلسطينية، وإيصال خطابها الى دائرة واسعة، بعيداً عن ممارسات التشويش والتزوير التي تمارسها آلة الاعلام الصهيوني، وتوفير قنوات إضافية لدعم الحركة، وزيادة حجم التنسيق بين أعضائها، وتوفير دعم مالي، ولوجستي، بعيداً عن القيود التي يفرضها الحصار الدائم على قطاع غزة.

ويمكن إجمال الإطار العام لسياسة الحضور السيبراني لحركة حماس بالمحاور الآتية (*Hanna,2006*):

محور المعلومات والاتصالات: تسخير القدرات التي توفرها شبكة الانترنيت ومواقعها، للتنسيق بين أعضاء الحركة، وتبادل المعلومات الحساسة، وتشفير محتوى الخطاب الذي يتداولها أعضاءها، والتواصل مع أنصار الحركة، متجاوزة عقبة التباعد الجغرافي، وصعوبة التواصل نتيجة الإجراءات الأمنية المشددة التي تتبناها الحكومة الإسرائيلية لكفّ أنشطة الكفاح الفلسطيني.

المحور الثاني: الدعاية والاعلام الموجّه: أثبت المركز الفلسطيني قدرته المميزة في نشر خطاب إعلامي رصين، ونجح، بفضل الخدمات الإعلامية التي توفرها مواقع الويب، وشبكات التواصل الاجتماعي، في تحقيق تواصل بناء للحركة داخل حدود الوطن العربي، واقليمياً، ودولياً وكسب المزيد من الأنصار للحركة، وتسفيه خطاب آلة الاعلام الصهيوني، بعد أن استطاع تحقيق بثّ حي للوقائع من أرض القطاع، والضفة، يظهر بجلاء الانتهاكات الصهيونية، مما أوقع الأعداء في حرج شديد، وأجبرهم على تغيير الكثير من مفردات سياستهم الإعلامية المضللة.

المحور الثالث: تمويل الحركة من الدعم المالي الذي يوفره أنصارها بعيداً عن قيود الرقابة المالية الذي باتت تفرضه المؤسسات المصرفية على تدفق الأموال، وعبر حسابات مالية تبتعد عن أنظار المؤسسة الصهيونية. فنجحت الحركة بفتح قناة مباشرة، وآمنة مع الأفراد والمؤسسات لتوفير دعم مالي مستمر.

المحور الرابع: تجنيد أعضاء وأنصار جدد للحركة داخل حدود الأرض المحتلة، وخارجها، من خلال قنوات مواقع الويب، وشبكات التواصل الاجتماعي.

المحور الخامس: تحويل جزء لا يستهان من كفاحها ضد الكيان الصهيوني الى فضاء يخلو من الاحتكاك، ولا يفتقر الى دعم لوجستي كبير، مع توسيع نطاق المواجهة بحيث يمكن أن يشارك أي فلسطيني، أو عربي، أو نصير من أنصار الحركة في دعم الكفاح الفلسطيني، بصورة مباشرة من خلال فضاء الفيض السيبراني، بوصفه مجالاً جديداً لممارسة أنشطة الكفاح الفلسطيني باستهداف مواقع العدو الصهيوني، وتخريب وخلخلة أداء مواقع الحكومة الإسرائيلية، والضغط على الآلة الاقتصادية، وسوق الأوراق المالية. وقد وسّع من دائرة استثمار قدرات شبكة الانترنيت بعد أن خطا نحو توظيف شبكات التواصل الاجتماعي، التي لم يعد الانسان المعاصر قادراً على مغادرة مواقعها ببث خطاب موجّه يعمّق آثار حرب نفسية من نمط جديد، بات يؤثر على المواطن الصهيوني، ويورث الحكومة الإسرائيلية قلقاً مضاعفاً.

5 . 3 . 2 . مراتب الحضور السيبراني لحركة حماس على مواقع الويب:

تظهر عملية تحليل الحضور السيبراني لمواقع الحركة المختلفة أن المجتمع الافتراضي الجهادي *Virtual Jihadi Community* لحركة حماس يتألف من مجموعة متنوعة من مواقع الويب، والمنتديات، والمدونات التي تشرف الحركة على إدارة عملها، وتغذيتها باستمرار بخطابها السياسي، والثقافي الذي يصبّ في القضية الفلسطينية وتداعياتها المختلفة.

وتتوفر أمامنا أكثر من طريقة لتصنيف عناصر البيئة السيبرانية للحركة، بيد أننا سنحاول أن نتعامل مع هذه المواقع بنفس الطريقة التي تتبناها مراكز البحوث التي تعنى بدراسة هذا النمط من المواقع(*NCTB,2007*).

ورغم أنه لا يمكننا أن نضع حداً فاصلاً تتحدد من خلاله بدقة، طبيعة الأدوار التي تمارسها مواقع حماس على الانترنيت، نتيجة لوجود تداخل في ممارسة الأدوار بالموقع ذاته، بيد أن التصنيف العام لهذه المواقع سيجعلنا قبالة الأصناف الآتية لمواقع الويب:

1. المواقع الرسمية للحركة.
2. مواقع التيارات الأصولية لحماس.
3. مواقع ثانوية ومنتديات.
4. قنوات التوزيع.

تنضوي المواقع الرسمية لحركة حماس ضمن موقع المركز الفلسطيني للإعلام الذي قد سخرته الحركة ليعبّر عن موقفها الصريح إزاء أهم مسائل قضية الصراع الفلسطيني ـ الإسرائيلي بأبعادها السياسية والدينية والحضارية، من خلال لسان حال المقاومة، والحماسة، والجهاد.

تأسس الموقع في بداية شهر نوفمبر من عام 1998، وبدأ بممارسة نشاطه الإعلامي / السيبراني في مارس من عام 1999. وتحرص الكوادر السيبرانية للحركة على وجود موقع مرآة (عدة نسخ من الموقع) لتجاوز الإشكاليات التي قد تنشأ عن الهجمات السيبرانية التي يمارسها الكيان الصهيوني وأنصاره على الموقع بقصد تخريبه، أو كف أنشطته الإعلامية المعادية للصهيونية، بحيث يمكن إعادته للعمل من مجهزات خدمة الانترنيت.

استثمرت حركة حماس سهولة التواصل عبر مواقع البريد الالكتروني، ومواقع الويب، وحسابات شبكات التواصل الاجتماعي لتوفير تمويل من الجهات الداعمة للحركة. وقد وفرت دعم فني لإرشاد المتبرعين حول كيفية تجاوز عقبة المراقبة الأمنية الصارمة التي تفرضها بعض الحكومات، وذلك عن طريق استخدام أسماء مستعارة، عند التواصل برسائل البريد الالكتروني (*Jacobson,2009*).

وتلتحق بقنوات التوزيع مواقع التواصل الاجتماعي، التي بدأت تنمو بصورة متسارعة خلال السنوات الخمس الأخيرة، ومواقع مشاركة الملفات الفيديوية مثل: *YouTube* وإن لم تنتمي بصورة مباشرة الى مواقع الحركة، كونها تشكل فضاءً معلوماتياً مضافاً تستودع فيه مادة إعلامية تدعم نشاط الحركة، من خلال الخطاب الإعلامي الذي يقطن في مادة وسائطها المتعددة.

وتتوفر عدة منتديات معلوماتية بعضها ينتمي الى حماس (مثل:*The Gaza Hacker Team Forum* ، و*Palestinian Anger Forum*)، وأخرى تعود لمجاميع قراصنة عرب (مثل:*The Arabic Mirror Forum*) يعكفون على توفير الدعم العلمي، والتقني، واللوجستي للأفراد والجماعات التي تمارس الهجمات والتهديدات السيبرانية ضد مواقع الكيان الصهيوني، والشركات الإسرائيلية، أو الغربية التي تدعمها (*Carr,2012*).

بالمقابل شجعت النتائج المبهرة التي حققتها شبكات التواصل الاجتماعي في إذكاء ثورات الربيع العربي، دول شمال أفريقيا، وسوريا حركة حماس على التوجه صوب توظيف تطبيقات منصة شبكات التواصل الاجتماعي (*Twitter،Facebook*) ضمن ادواتها السيبرانية المقاومة للاحتلال الصهيوني.

وبدأت الإدارة السيبرانية في الحركة بإنشاء مواقع للتواصل الاجتماعي، والتغريد السيبراني، تناظر تلك التي استوطنت مواقع الويب منذ بدايات الألفية الجديدة، وبدأت باستثمار قدراتها الاتصالية، وبيئتها التواصلية الحميمة، في كسب المزيد من الأنصار، والجهات التي تتعاطف مع الكفاح الفلسطيني وتشجب بشدة الإجراءات التعسفية، والعدوان العات الذي تمارسه الآلة العسكرية الاسرائيلية الغاشمة التي باتت تحصد أرواح الفلسطينيين بدون أدنى رحمة.

وقد وسّعت الحركة دائرة حضورها التواصلي بزج المؤثرات المرئية، فقام المكتب الإعلامي لحماس بإنشاء موقع يحاكي الدور الذي يمارسه مواقع التواصل الفيديوي *YouTube* بتاريخ 12-10-2008 وأطلق عليه اسم موقع *Aqsa Tube* وأودع فيه ملفات فيديوية للهجمات والانتهاكات الإسرائيلية في غزة المحتلة (*IDF,2008*).

ثم باشرت بإنشاء حسابات للحركة، وأخرى لآلتها الإعلامية، وبعض قياداتها على منصة شبكات التواصل الاجتماعي، فوسعت من نطاق نشاطها الإعلامي، وبث اخبار الحركة، بصورة آنية وتفاعلية، من داخل القطاع. واستطاعت حركة حماس أن ترسخ حضورها، ضمن حسابات منصات شبكات التواصل الاجتماعي، مثل: *Twitter ،Facebook*، قنوات *YouTube*، وصفحات موقع *Google+*، وغيرها من منصات التواصل الاجتماعي لتلافي قيام مجهزي الخدمة واستضافة المواقع بإغلاق مواقعها على صفحات الويب.

من جهة أخرى تعد قناة انتفاضة فلسطين من قنوات موقع التواصل المرئي *YouTube*، وترتبط مع حسابات كتائب القسام على موقع *Twitter* ، وتعمل مستقلة عن قناة المركز الفلسطيني للإعلام التي تمتلك موقعاً مستقلاً على موقع *YouTube*. ويكاد يتوافق المحتوى المطروح على حساب عزة الرشيق في كل من موقعي *Facebook*، و*Twitter*، ويتواصل بارتباطات حميمة مع حسابات كتائب عز الدين القسام.

وتمتلك وكالة الرأي للإعلام، حساباً على موقع *Facebook*، واخر على موقع *Twitter*، وآخر على موقع *YouTube*، يضاف إليهم موقعها المميز على منصتي برمجيات *ITunes* و*Play Google* اللذان يوفران تطبيقات على الحواسب اللوحية، والهواتف الذكية للتواصل مع هذه الوكالة، وحساباتها المتعددة.

ونلاحظ بالوقت ذاته كثرة المدونات السيبرانية المناصرة لحركة حماس، والقضية الفلسطينية، والتي تستمر بنشر النصوص التي تنافح عن حركة حماس، وتناهض خطاب الاحتلال الإسرائيلي. وقد أظهرت تحرياتنا الأولية أن عدد المدونات التي كرست خطابها المدون لدعم حماس قد بلغ 22 مدونة، بينما ناهز عدد المدونات التي تدعم القضية

الفلسطينية حوالي 12 مدونة، وبلغ عدد المدونات المتعاطفة مع القضية 10 مدونات، وعثرنا على 7 مدونات شخصية يصب خطابها في دعم كفاح حركة حماس ضد الكيان الصهيوني.

5 . 3 . 3 . السلطان السيبراني لحركة حماس في الفضاء السيبراني:

في البداية انصب اهتمام الحركة على المحور الإعلامي والسياسي فاستثمرت ظاهرة الانفتاح العولمي لفضاء الفيض السيبراني في ينشر خطاب المقاومة للحركة وكسب المناصرين والمتعاطفين من داخل حدود الوطن العربي وخارجه.

وبدأت بوادر السجال السيبراني بين أنصار الحركة وأنصار الكيان الصهيوني باستهداف مواقع الويب لهذه الجهة أو تلك، دون أن يكون للحركة بصمة واضحة تؤشر نحو دور ملموس على صعيد المدافعة أو شن الهجمات. بيد أن تطور النزاع السيبراني مع بداية الألفية الجديدة، وكثرة الهجمات التي استهدفت مواقع الحركة، من جهة، وتوجه الأنظار نحو إمكانية استخدام فضاء الفيض السيبراني بوصفه ساحة مواجهات ومنافحة افتراضية بين الكيانات المتصارعة على أرض الواقع قد جذب انتباه كتائب عز الدين قسام ـ الذراع العسكري للحركة نحو تشكيل فصائل رقمية تباشر ممارسة التهديدات والهجمات السيبرانية على مواقع الكيان الصهيوني.

وقد وجدت الحركة في الخبرات التي تمتلكها فصائل حزب الله، والدعم التقني واللوجستي الذي توفره إيران ملاذاً مهماً لتطوير وبنات قدرات كوادرها السيبرانية، وتوظيف الأدوات التي يمكن أن يوفرها النظام الإيراني كجزء من الدعم لمن ينافح ضد الكيان الصهيوني بالمنطقة.

فولد كيان رقمي جديد بات يعرف بفصائل عز الدين قسام السيبرانية في بداية العقد الأول من الألفية الجديدة، وبات يشارك في شن هجمات على مواقع الكيان الصهيوني، ليشكل تهديداً مضافاً مع التهديدات والهجمات التي تمارسها فصائل حزب، والتي تنتظم جميعاً ضمن أهداف النظام الإيراني في تأجيج الصراع مع إسرائيل (*Hp,2014*).

ورغم أن الهجمات وعمليات القرصنة السيبرانية، كانت في بداياتها، بدائية، وتفتقر الى التنسيق، وتستخدم أدوات تتوفر في مواقع الانترنيت، أو منتديات القرصنة، إلا أنها قد تطورت شيئاً فشيئاً فأمست أكثر تطوراً، (بفضل الدعم التقني الذي توفره إيران بصورة مباشرة أو بالتنسيق مع الفصائل السيبرانية لحزب الله اللبناني) وبدأت بتوظيف أدوات قرصنة نجح بإنشائها مجاميع قراصنة عز الدين قسام وانصارهم، مما دعم تغلغلها الى البنى التحتية السيبرانية لإسرائيل، فأصبحت أكثر تأثيراً وإيلاماً، بعد أن استطاعوا اختراق الكثير من الحسابات المصرفية، وكشف بيانات مهمة عن بضعة مئات الألوف من بطاقات الائتمان، وخلخلة عمل سوق تل أبيب للأوراق المالية، مما نجم عنه حصول انخفاض بلغ 8% بالأسهم الإسرائيلية. وقد وسعوا نطاق هجماتهم التي تحولت نحو فضاء شبكات التواصل الاجتماعي، فبدأوا بالضغط على كثير من المؤسسات العسكرية والأمنية، وبلبلة الرأي العام الإسرائيلي أثناء جريان العمليات العسكرية.

5 . 4 . جيش فضاء اليمن السيبراني (YCA) *Yemen Cyber Army*:

ولم يبرز جيش فضاء اليمن السيبراني على سطح الحدث في الفضاء السيبراني العولمي قبل عام 2015، وبالتحديد في شهر أبريل، وارتبطت واقعة حضوره بالمواجهات العسكرية التي استعرّت بين دول التحالف العربي، بقيادة المملكة العربية السعودية والميليشيات المسلحة للحوثيين ومن التحق بها من قوات الرئيس اليمني المخلوع علي عبد الله صالح.

وليس ثمة معلومات أكيدة حول الهوية الحقيقية لأفراد هذا الجيش السيبراني سوى مناصرته ومنافحته عن حركة الحوثيين في اليمن، وولائه المطلق لخطاطة الثورة الاسمية في إيران، وتحالفه مع فصائل حزب الله اللبناني، ومعاداته وخلافه مع النظام السعودي وحلفائه الذين التحقوا بركب التحالف العربي.

ويدّعي الناطقون بلسان هذا الجيش السيبراني أن مستقر قيادته في اليمن، بينما تؤكد المصادر أن عنونة موقعه في فضاء الانترنيت تنتمي الى فضاء إيران السيبراني، كما أن لغة الخطاب والتواصل بين أفراده هي اللغة الفارسية، الأمر الذي يؤيد تهافت هذا الادعاء ويساند فرضية أن هذا الجيش المتخيل لا يعدو عن كونه فصيلاً من فصائل قوات الردع السيبراني الإيراني، أو الجهات والوكلاء السيبرانيين الموالين لها قد التحق به بعض قراصنة المعلومات المحليين ممن يقيمون داخل حدود اليمن أو من المغتربين خارج حدوده (*Bicchirea,2015*).

وقد ظفر فريق *The Intelligence* الأمريكي، والمتخصص بشؤون قراصنة المعلومات بأدلة تشير الى وجود تحالف وشراكة وطيدة بين قراصنة معلومات من اليمن مع مجاميع قرصنة إيرانية مثل مجموعة *Parastoo* الشهيرة ومجموعة أخرى أطلقت على نفسها اسم *EMAD* (*Crowdstrike,2015*).

ويكاد يجزم الكثير من خبراء أمن المعلومات في دول المنطقة، ودول أوربا، والولايات المتحدة أن جيش فضاء اليمن السيبراني ليس سوى واجهة تتخفى وراءها فصائل متعددة من قوى الردع السيبراني الإيراني، والتي تنفذ سياسة النظام الإيراني وحرصه على النهوض بمهمة المدافع الأول عن حقو الشيعة في العالم الإسلامي، وبسط نفوذه بالمنطقة، وتعويض المعادلة غير المتوازنة للقوى بمنطقة الخليج العربي نتيجة للتدخل العسكري لدول التحالف العربي في الملف السياسي لليمن[188].

---

[188] . ولعل من الأدلة المتكاثرة حول انتماء هذا الجيش السيبراني الى إيران ومحاولة صبغه بصبغة يمنية (*Bicchirea,2015*):

- عدم رسوخ قدم اليمنيين في مجال القرصنة السيبرانية، وعدم وجود ملفات تثبت حضور مثل هذا النشاط قبل ولادة الجيش السيبراني.
- ترويج الاعلام الإيراني لنشاطات القرصنة التي يمارسها أفراد هذا الجيش، وبصورة حصرية في كثير من الأحيان.
- العثور على وثائق في موقع هذه المجموعة تعد من الوثائق الحصرية لمجموعة قراصنة *Parastoo* الإيرانية الشهيرة.
- عدم وجود بصمة حضور لأعضاء هذه المجموعة، أو أفراد الجيش على فضاء التواصل الاجتماعي، والذي يعدّ شاهداً اكيداً على حضوره في فضاء اليمن السيبراني، شأن الجيش الالكتروني السوري *SEA* وفصائل حزب الله اللبناني، وفصائل عز الدين قسام السيبرانية في غزة.

الفصل السادس:
السجال السيبراني بين إيران وخصومها في فضاء النزاع السيبراني

الفصل السادس: السجال السيبراني بين إيران وخصومها في فضاء النزاع السيبراني

1. إعادة تشكيل آلية توازن القوى في فضاء الفيض السيبراني:

أسهمت مجموعة الخصائص الفريدة التي يتسم بها فضاء الفيض السيبراني في إعادة تشكيل آلية توازن القوى بين الجهات المتصارعة نتيجة لتداخل الخاصية المتخيلة مع مفردات الواقع الصلبة، وتراجع كلفة الولوج الى مجال الفضاء المتخيل، وسيادة ممارسة استعارة هوية الحضور *Anonymity*، مع غياب سمة التوازن والتناسق *Asymmetries* في إدارة الصراع وتحديد مستويات التأثير *Vulnerability* ، الأمر الذي غيّب خاصية التوازن بين الفاعلين الكبار (الدول أو المؤسسات التي تمارس العمل العسكري) من جهة، وبين الفاعلين الصغار (مجاميع قراصنة المعلومات والمستخدمين العاديين) أثناء حدوث صراع داخل حدود الفضاء المتخيّل، توسيع رقعة التهديد أو باتجاه كيانات تقيم في فضاء حياتنا اليومية، من جهة أخرى (*Nye,2010*).

لقد أسهم الفضاء السيبراني في تقليص الفوارق بين موازين القوى التي ترسّخت لدينا (عند مراجعة هوية الجهات المتصارعة)، فلم تعد القدرة على إحداث الضرر في أحد الخصوم مرتهنة بالموازين التقليدية لأن الخصوم الصغار (مثل قراصنة المعلومات) أصبحوا بفضل ما يتسم به الفضاء السيبراني من مميزات فريدة، قادرين على إحداث ضرر في لاعبين كبار على مستوى الحكومات أو الدول الأربع الكبرى (على سبيل المثال) وبمستويات لا يمكن أن تقارن بالأثر المعكوس الذي ينتج عن استجابة هذه الدول وتعاملها مع موارد التهديدات. لقد مزّقت خطاطة فضاء الفيض السيبراني مفاهيمنا لتوازن القوى وآلية سريان القوة المؤثرة بنفس الطريقة التي مزّقت بسمتها الافتراضية المتخيلة خاصية المكان، وغيّبت مفهوم الإزاحة المكانية وارتباطها بعنصر الزمان، وأتاحت الفرصة لحضور متعدد في الفضاء ذاته، وخلال بعد زمني متقارب جداً.

ولم تعد حوكمة مجال النزاع بيد جهة دون غيرها، ومهما كان مستوى السطوة التي تتمتع بها داخل حدود الفضاء المتخيّل، أو خارجه، ذلك لأن حضور الفرق، والجماعات، والمجتمعات المتخيّلة *Virtual Communities* أصبح خارج نطاق سلطة الغير، وبعيداً عن مجال هيمنة المتنازعين في كثير من الأحيان. لقد تلاشت المعمارية الهرمية التي طالما حكمت مجال المنازعة، وبرزت بدلاً عنها المعمارية الشبكاتية ذات الوصف المكاني المنبسط، فغيّبت هيمنة الكيانات العملاقة بعد أن حوّلتها الى عقد رقمية تنتشر أفقياً على بساط النسيج الشبكاتي العولمي. فأضحت حوكمة مجالات الفضاء المتخيّل مرتهنة بخطاطات الجماعات المتخيّلة، بعيداً عن القولبة الضيقة للانتماءات القومية، والسياسية، والجغرافية.

لذا فإن عملية تحديد معالم توازن القوى التقليدية لم تعد سارية المفعول (في المجال السيبراني الجديد) بعد أن فرض فضاء الفيض السيبراني خطاطته الفريدة، والتي أسهمت في قلب مبادئ توازن القوى، وغيّرت هوية العوامل الحاكمة على صعيد تحديد مجال تأرجح كفة القوى المتصارعة.

2. الحرب الناعمة: بوابة ولوج إيران الى فضاء المنازعة السيبراني:

لم تشكّل الإنترنيت هاجساً امنياً كبيراً لدى المؤسسة الأمنية الإيرانية، في بداياتها، فتعاملت معها شأن منافذ الإعلام العولمي حيث تمارس عمليات الكف والحظر على المحتوى السيبراني الذي يحمل في طياته خطاباً مناهضاً للنظام الإيراني وممارساته القمعية.

ومع بزوغ الحركة الخضراء عند حملة انتخابات عام 2009 الرئاسية، وتدفق السيل الهادر من الخطاب المعارض للنظام ومنظومتيه الأمنية والعقدية، استشعر النظام بدءاً بالمرشد الأعلى مدى خطورة تطبيقات منصات التواصل الاجتماعي وقدرتها على إحداث تغيير حاسم في التركيبة السياسية بواسطة آليات ناعمة، وبعيداً عن آلة العنف التي يحسن النظام استخدامها مع معارضيه.

فنشب عن المناخ الذي تولّد نتيجة للأحداث الساخنة والمتلاحقة خلال تلك السنة، بروز توجه جديد لدى النظام الإيراني تجلى بسلسلة الخطابات التي ألقاها المرشد الأعلى للثورة علي خامنئي منذراً قيادات الثورة وجماهيرها من الأخطار المحتملة لحرب جديدة تحاول خلخلة الرأي العام الإيراني، تمهيداً لزحزحة النظام عن مساره، وأطلق عليها اسم الحرب الناعمة.

لقد ولج النظام الإيراني في ساحة مواجهة من نمط جديد، تدور رحى منازلتها في فضاء متخيّل، وتوظف أدوات وآليات جديدة، بدأت بالتخطيط للحصول عليها، وإحسان استخدامها، وانتخاب خطط رشيدة للدفاع عن حياض البلاد، وممارسة هجمات ناعمة على خصومها العنيدين.

2 . 1. الحروب الناعمة: مراجعة مفاهيمية:

ولد اصطلاح السلطة الناعمة *Soft Power* للمرة الأولى ضمن الكتاب الذي أطلقه الباحث الأمريكي *Joseph Nye* من جامعة هارفارد، عام 1990[189]، في محاولة لدعوة الإدارة الأمريكية لتغيير مسارات سياساتها والتوجه صوب سلطة من نمط جديد تضمن ريادتها وهيمنتها العولمية. ثم لم يلبث أن عاود مراجعة مفهوم المصطلح الجديد في كتاب آخر[190]، صدر عام 2004 ليتوافق مع الحضور الهادر لتقنية المعلومات وأدواتها ويستثمرها لبسط السلطان الجديد في الفضاء المتخيّل وفضاء الواقع(*Wikipedia,2016*).

لم يتسم التعريف الذي طرحه ناي، في بداياته، بسمة التعقيد، بل كان مباشراً، فعدّ السلطة الناعمة نهجاً بديلاً للسلطة الصلبة *Hard Power* حيث تستخدم سلطة الإقناع، والجذب لانتزاع الخصم من هيمنة القيم السياسية، والعقدية، والثقافية التي تغلغلت في نسيج حياته باتجاه قناعات مصطنعة تصطنع بواسطة قنوات تتخفى وراء الشفافية التي تفتعلها مؤسسات حكومية ومنظمات سخّرت لهذا الغرض.

[189] . عنوان الكتاب الأول: *Bound to Lead: The Changing Nature of American Power.*

[190] . عنوان الكتاب الثاني: *Soft Power: The Means to Success in World Politics.*

وقد استوطن اصطلاح الحرب الناعمة في خطابات المرشد الأعلى للثورة قبل بقية القيادات، فحذّر من مغبة ممارساتها بكثافة ضد الثورة الإسلامية بعد الحملة الانتخابية الرئاسية عام 2006 (الزين،2011). فأطلقه في عدد كبير من خطاباته ولقاءاته مع القيادات أو الشبيبة الإيرانية الملتزمة بالخطاب العقدي للثورة[191].

لقد أكد المرشد الأعلى للثورة على وقوع الحرب الناعمة في فضاء الواقع الإيراني (حمدان، 2010)، وحذّر من استمراريتها، وإ مكانية الوقوع في شراكها الخفية، داعياً الى ابتكار سبل جديدة لمواجهتها، ومقاومتها، وعظّم من شأنها حتى عدّها التهديد الرئيسي للثورة الإسلامية، ووجه دعوته الى الجامعيين والشباب أن يكونوا ضباطاً للحرب الناعمة، وتوقع أن ميدان المنازلة الجديدة مع قوى الشر (بحسب قوله) سيكون في ميدان الحرب الناعمة، والتي وصفها بأنها حرب عسكرية تخوضها الثورة الإيرانية ضد خصومها (مركز الحرب الناعمة للدراسات،2014).

وقد ربط *Joseph Nye* القوة الناعمة بالقدرة الكامنة لدى أمة من الأمم بالتأثير في أمم أخرى وتوجيه مسارات حزمة من خياراتها العامة نتيجة للجاذبية التي يتمتع بها نظامها المعرفي والاجتماعي والسياسي حيث يغيب عنها نهج الإكراه والتهديد لتحل محله قيم الحرية والقبول الطوعي بمجالات الأمور على ساحة الحياة اليومية بمختلف تفاصيلها ومحاورها (ناي، 2004).

وعلى نقيض القوة الصلبة الغاشمة التي تفرض خطاطة الأمة المتغلبة على غيرها بالقوة والإكراه، فإن القوة الناعمة تتسلل خلسة إلى نفوس أفراد الأمة المغلوبة فيهرعون إلى ممارسة خطاطتها دون أن تلتفت نفوسهم الى أهدافها المستبطنة مع غياب الإحساس بالإكراه على ممارستها.

وتكاد تتناسب القوة الناعمة بنهج عكسي مع القوة الصلبة إذ كلما تعاظمت الأولى تراجعت الثانية وانتفت الحاجة إلى توظيف آلتها الصلبة التي تكلف المال الجم والقوة القاهرة، بينما لا تفتقر الأولى إلى مثل هذه الموارد، وتوظف مبدأ الأنموذج الجاذبية لضمان بسط سلطانها[192] (عبد السلام، رفيق، 2008).

2 . 2 . رؤية المرشد الأعلى وعنايته بمفهوم الحروب الناعمة ومجالاتها:

ولدت رؤية المرشد الأعلى للثورة الإيرانية، حول الحروب الناعمة، ونضجت، بعيد المواجهات التي نشبت بين المعارضة الإيرانية والنظام أثناء الحملة الانتخابية الرئاسية، وبروز أدوات وتطبيقات شبكات التواصل الاجتماعي بوصفها أدوات دعم لوجستي لتوسيع نطاق المواجهة، وبسط خطابها داخل حدود إيران، وخارجها.

وعدّ حملة الدعم الذي وفرته الإدارة الأمريكية لضمان استمرار عمل منصات التواصل الاجتماعي (ورغم حرص الإدارة الحكومية الإيرانية على ممارسة عمليات الكف والحظر على هذه المواقع، وتوفير بدائل اتصالية للمعارضة)

---

191 . بلغ عدد الخطابات واللقاءات التي ذكر فيها الامام علي خامنئي هذا الاصطلاح خلال المدة بين 12 حزيران عام 2009 لغاية شهر شباط من عام 2014 أكثر من مناسبة بحسب ما أحصاه مركز الحرب الناعمة للدراسات (مركز الحرب الناعمة، 2014).

192 . قد عزى مركز الحرب الناعمة للدراسات (الذي يستوطن العاصمة اللبنانية، بيروت، ويلقى دعماً من النظام الإيراني) توجه الولايات المتحدة المكثّف نحو توظيف آليات الحروب الناعمة نتيجة للإخفاقات المتكررة التي تعرضت إليها حملاتها العسكرية في أفغانستان والعراق بعيد عام 2006، لتقليل حجم الانفاقات وتقليص خسائرها البشرية في المواجهات العسكرية على الأرض (مركز الحرب الناعمة للدراسات، 2014).

محاولة مكشوفة لشن حرب ناعمة ضد خطاطة النظام، والسعي الى تفكيك النسيج المتماسك للشعب الإيراني، وتوسيع هوة الخلاف بينه وبين خطاب الثورة الإسلامية بالبلاد (مركز قيم للدراسات، 2011).

وبدأ بالتأكيد على مبدأ التهديد الجديد، وحذّر من عواقبه الخطيرة على خطاطة الثورة الإسلامية، ومستوى توطنها في نفوس الشعب الإيراني، وبدأ بقرع ناقوس الخطر، في الكثير من خطاباته ولقاءاته العلنية، منذراً من محاولات تفكيك النسيج الإيراني المتماسك، بنهج غير معلن، وآليات غير تقليدية.

وقد هرعت المؤسسات الثقافية التي تمارس نشاطها في لبنان، برعاية مباشرة من حزب الله وبدعم مالي إيراني بتأسيس مركز الحرب الناعمة للدراسات[193]الذي هرع الى إصدار الكثير من الدراسات والكتب التي عالجت المسألة من جوانب متعددة[194].

وقد ترجم موقف المرشد الأعلى من الحروب الناعمة عبر سلسلة من الإجراءات التي تولدت عنها الاستراتيجية السيبرانية الإيرانية خلال السنوات التي تلت الحملة الانتخابية، واتسمت بتوجهات نحو حماية البيئة السيبرانية ـ الإيرازية من تهديدات الحروب الناعمة مع تسخير الآلة الإعلامية للثورة الإسلامية في درء الخطاب التحريضي، وبثّ الوعي على المستوى الجماهيري.

بيد أن الهجمة الشرسة لفايروس *Stuxnet* على المشروع النووي الإيراني، قد أحدثت انعطافاً مفاهيمياً لدى النظام الإيراني، فوسّع من مجالات سوح المواجهة للحروب الناعمة وبادر الى إنشاء المزيد من مراكز الدفاع والردع السيبراني الإيراني، لتعزيز حصانته ضد التهديدات الجديدة.

2 . 3 . التمييز بين مفاهيم مختلطة:

هرعت القيادة الإيرانية الى توظيف مصطلح الحرب الناعمة قبل أن تتحدد دلالته وتتضح مجالاته، بحيث حصل تداخل مفاهيمي بين حرب الإعلام المضاد الذي مورس منذ عقود متطاولة، وبين الحروب والمواجهات التي تنطلق في فضاء المنازعة السيبراني، وحملات الإعلام المضاد وخطاب المعارضة الذي انتشر داخل حدود فضاء منصات فضاء التواصل الاجتماعي، بشكل غير مسبوق خلال عقد من الزمان.

لقد ولد اصطلاح السلطة الناعمة لدى الكاتب الأمريكي *Joseph Nye* في عقد التسعينات من القرن العشرين، وقبل أن نشهد ولادة منصة تطبيقات شبكات التواصل الاجتماعي، بينما عمد المرشد الأعلى للثورة الإيرانية الى التنبيه من

193 . كشف مركز الحرب الناعمة للدراسات عن هويته في موقعه الإلكتروني بأنه مركز علمي بحثي واستشاري يُعنى بالأبحاث والدراسات ذات العلاقة بالحرب الناعمة محاولاً الإضاءة عليها والتركيز على القيم التي تنشر بواسطتها بهدف تحصين المجتمع والمواجهة على المستويات الثقافية والتربوية والإعلامية. وبيّن أنه يتبنى في عمله نهجاً مؤسساً على ممارسات علمية بحثية، بقصد التعمق في دراسة الظواهر القيمية التي تغزو المجتمع بالأخص على مستوى الأسرة والناشئة تمهيداً للمعالجة الجذرية للمشاكل بما يساهم في تحصين مجتمع المقاومة من القيم الواردة. وربط أهدافه برصد الظواهر والمستجدات في مجال الحرب الناعمة وأدواتها ووسائلها بالأخص الظواهر التي تترك آثاراً سلبية على المجتمع، وإنتاج الأبحاث والدراسات النظرية والميدانية حول الحرب الناعمة وأبعادها بما يلبي الاحتياجات المطلوبة، وتقديم الاستشارات والاقتراحات حول صناعة ومواجهة الحرب الناعمة، وتعزيز العلاقة والتعاون من المؤسسات الثقافية والفكرية بما يؤدي الى تحصين المجتمع من آفات الحرب الناعمة، وأخيراً نشر الوعي حول خطورة الحرب الناعمة وخطورة أدواتها ووسائلها، مستمداً مبادئه وقيمه من نهج قائد الثورة الإسلامية الإمام الخميني، والمرشد الأعلى للثورة الإسلامية علي خامنئي.

راجع موقع المركز: *http://www.softwar-lb.org/*

194 . نذكر منها: الحرب الناعمة: معالم رؤية الإمام الخامنئي، ورؤية الإمام خامنئي في مواجهة الحرب الناعمة.

مخاطر القوة الناعمة وحروبها بعد أن نجحت المعارضة الإيرانية في بث خطابها المعارض أثناء الحملة الانتخابية الرئاسية في الفضاء السيبراني المتخيّل عام 2009 (*Price,2012*).

كذلك فإن القوة الناعمة لدى منتج مصطلحها كانت حكراً على الدول الكبرى، التي تمتلك قيماً وممارسات جاذبة للشعوب المقهورة لخلق فضاء محلي يحاكي اليوتوبيا المفترضة، غير أن ما أقلق المرشد الأعلى هو تعاظم سطوة الخطاب المعارض للثورة الإسلامية، وبداية حصول انشقاقات في النسيج المجتمعي الإيراني بواسطة أدوات لينة *Soft Tools* لم تعد تجدي سطوة الأدوات الصلبة (التي تمتلكها المؤسستين الأمنية والعسكرية الإيرانية) *Hard Tools* في مواجهة فيضها السيبراني الهادر.

ويضاف الى كل هذه الأمور المستحدثة أن استخدام المعارضة الإيرانية للأدوات السيبرانية، وتسخير تطبيقات التواصل الاجتماعي لبثّ خطابها، لم تحاكي ممارسة مشابهة لدى الدول والنظم المناهضة لإيران، بل كانت سابقة جديدة شدّت انتباه المؤسسات المنتجة لهذه الأدوات والإدارة الأمريكية الى السطوة التي تستبطن في هذه الأدوات، وفرص استثمارها في قضّ مضاجع النظام الإيراني بعيداً عن استخدام السطوة الصلبة وتحمل أعباءها المالية الباهظة.

من أجل هذا آثرنا استخدام اصطلاح القوة اللينة بدلاً من القوة والحروب الناعمة للتمييز بين ممارسات الجذب التي تمارسها النماذج التي تصطنعها الدول المتغلبة مثل الولايات المتحدة الأمريكية حول قيمها وممارساتها الاجتماعية وتحاول وسمها بصبغة مثالية جاذبة، وبين الأنشطة التي تمارس في الفضاء السيبراني المتخيل، وأدواتها اللينة *Software* في ممارسة الضغوط، والتهديدات على نظم متسلطة.

ورغم عدم تطابق دلالة مصطلح الحروب الناعمة لديها مع ما يحصل في فضاء المنازعة السيبراني المشحون بالتهديدات والهجمات السيبرانية فقد أسهم توظيف هذا المصطلح، وشغف المرشد الأعلى بمضامينه في توسيع دائرة اهتمام النظام الإيراني بمجاله، وتسخير الكثير من موارد إيران لضمان تعاظم السطوة الناعمة، قبل أن تتأكد زكانة المرشد الأعلى وتحذيراته المتكررة من خطورة الحرب الجديدة عندما نجحت الهجمة التي قام بها فايروس *Stuxnet* على أجهزة الطرد المركزي في المشروع النووي الإيراني، حينئذ لم يعد أمام الإدارة الإيرانية سوى البدء بخطوات متسارعة في التحضير للدفاع وممارسة عمليات الردع السيبراني لحماية الموارد المهمة، وحماية المشاريع الاستراتيجية بالبلاد.

3. السلطان السيبراني الإيراني: البدايات ومطالع النضوج:

إذا كان مفهوم السلطان (أو السلطة أو القوة) *Power* (وفق خطاطة مفاهيمنا التقليدية) عصياً أمام محاولات البيان والتبيين، فإن مفهوم السلطان السيبراني يعدّ الأكثر استغلاقاً أمام محاولات التفسير وبيان دلالاته الاصطلاحية (*Jordan,1999*).

فالسلطان أو الهيمنة قد توحي للوهلة الأولى، (دون الرجوع الى معاجم اللغة وقواميسها) الى استطاعة كيان من الكيانات وقدرته على ممارسة فعل يراد به تحقيق غاية تستبطن الرغبة بالغلبة، ضمن بيئة مشحونة بالتحديات.

أما إذا حاولنا توطين المصطلح في دائرة السياسة فستتحول دلالة المصطلح الى وصف قدرة كيان سياسي (دولة أو نظام إقليمي) على فرض جملة من الممارسات التي تؤثر على الخصم أو المنافس، وتفرض عليه أموراً قد تخالف توجهاته، أو غاياته، نتيجة للقوة القاهرة التي يمتلكها الطرف الأول في فرض أركان نفوذه (*Sheldon,2011*).

فعلى سبيل المثال، عندما أراد الباحث ناي توضيح دلالة مفهوم السلطان السيبراني، عمد الى تقسيم مجال فضاء الفيض السيبراني الى مجموعة من الطبقات التي تمارس خلالها مجموعة متعددة من الأنشطة التي توظّف الفضاء السيبراني وأدواته لاستثمار مادة الفيض السيبراني (التي تسافر في نسيجه الشّبكاتي) في إحداث تأثيرات متباينة في البنية التحتية أو عناصر الفضاء المتخيّل. وذهب الى أن شوكة هذا السلطان تعتمد الى حد كبير على هوية وقدرة الموارد السيبرانية التي تحدد خصائص مجال فضاء الفيض السيبراني (*Nye,2010*).

ولتبسيط هيكلة الأنموذج الهجين[195] (الذي اقترحه الباحث ليصف هذا المجال المعقد) افترض أن المجال يتألف من طبقتين، الأولى: فيزيائية *Physical* تتألف من عناصر وأدوات البنية التحتية للمعلومات والاتصالات. والثانية: متخيّلة *Virtual* تتألف مادتها من عناصر فضاء الفيض السيبراني وكياناته المتخيّلة ذات السمة الافتراضية.

بصورة عامة، تنصاع الطبقة الفيزيائية الى قوانين الطبيعة، وتحكمها خطاطة النظام الاقتصادي حيث تتدافع الموارد، وتتنافس لنيل فرصتها، مع ارتفاع كلف هذه الموارد في ظل هيمنة القانون على مجال هذه الطبقة. أما الطبقة الثانية فتمتلك خصائص الشبكة الاقتصادية حيث زيادة العوائد المتحققة مع توسع مجال التأثير، وصعوبة بسط هيمنة القانون على مجالها بسبب مرونته وانفتاحه بنسق يتناقض مع سمة الفضاء الفيزيائي المحكوم بعنصري المكان والزمان.

أما عملية ممارسة سلطان التأثير (الذي يروم بسط النفوذ، ومناكفة الخصم، والتزاحم على فضاء النفوذ) فترتكز الى مجموعة من الموارد التي تتسم بالمقدرة على تشكيل مادة فيض رقمي يتميز بصبغة اتصالية، وناقلية متميزة لمحتوى معلوماتي، قادر على إحداث تأثير معنوي على الغير، ضمن الطبقة ذاتها، او الطبقة الثانية اللذين يتكون منهما المشهد الكلي، الحاضن لجميع عناصر مجال المنازعة والمواجهة.

ويمكن، بعد أن نجري تعديلاً على هذا الأنموذج، أن نتوصل الى وصف جوهر السلطان السيبراني الإيراني، ومصادر قوة شوكته، وموارد غياب المنعة عن بعض مساحاته. وسيشمل التعديل الجديد إضافة حد فاصل بين القوة الناعمة والقوة اللينة واللتان قد لاحظنا اندماجهما لديه[196].

من أجل هذا عمدنا الى تمثيل معمارية السلطان السيبراني الإيراني بعد إعادة تشكيل بعض مفردات ومحاور أنموذج ناي، وحاولنا وصفها في الجدول (6 - 1).

[195] . تألف الأنموذج الذي اقترحه ناي من مجالين، فيزيائي يقيم في عالمنا الواقعي، وافتراضي *Virtual* يبسط حضوره في مجال الفضاء السيبراني المتخيّل. وجعل مستقر أهداف فرض السلطان السيبراني في منطقتين، الأولى: تستقر داخل الفضاء السيبراني، والثانية: تستوطن الفضاء التقليدي الذي يقع خارج الفضاء المتخيّل. أما بالنسبة للأدوات المستخدمة لفرض السلطان، فقد صنفها الى صنفين، أدوات معلوماتية، وأدوات فيزيائية، تمارس كل منهما تأثيراتها المعنوية على كلا المنطقتين. وعاد ثانية الى تقسيم الهجمات التي تمارسها هذين الصنفين من الأدوات الى قسمين، قسم يشمل هجمات لينة *Soft* وأخرى صلبة *Hard* (*Nye,2010*).

[196] . حاولنا التمييز بين استخدام اصطلاح القوة الناعمة الذي صرّح به قائد الثورة الإسلامية علي خامنئي، والذي يشمل جميع أشكال توظيف آليات المعلومات والاتصالات ومنصات التواصل الاجتماعي وتطبيقاتها في توجيه الرأي العام في الداخل والخارج، والتلاعب بعقول المستخدمين الإيرانيين لتحقيق غايات محددة، من جهة، والقوة اللّينة التي تستخدم كيانات الفضاء السيبراني الافتراضية في إنشاء تأثيرات ملموسة على الكيانات السيبرانية لدى الخصم دون توظيف خطاب سياسي كالذي يحصل في ممارسات القوة الناعمة.

الجدول (6 - 1) ـ معمارية وعناصر وآليات بسط السلطان السيبراني الإيراني.

طبيعة الأدوات والموارد المستخدمة	مواضع أهداف السلطان السيبراني			
	داخل فضاء الفيض السيبراني		خارج فضاء الفيض السيبراني	
	أهداف ليّنة	أهداف صلبة	أهداف ليّنة	أهداف صلبة
أدوات وآلات رقمية.	استهداف محتوى صفحات الويب. طمر فايروسات وديدان خبيثة. نشر محتوى رقمي معارض.	هجمات رفض الخدمة التي تتسبب بتوقف مواقع الويب عن العمل.	استخدام آليات الثورة الناعمة والديبلوماسية السيبرانية للتأثير على الرأي العام والضغط على النظام.	مهاجمة منظومات *SCADA* في مؤسسات نووية وأخرى صناعية. إحداث خلل في عتاد الحاسوب نتيجة لتأثير نمط محدد من الفايروسات.
أدوات وآلات فيزيائية.	جدران نارية ونظم مراقبة المحتوى وحظر مواقع.	فرض إجراءات مشددة على شركات تجهيز الخدمة والمقاهي الإلكترونية والشركات.	ممارسة وقفات احتجاجية لمناهضة حظر الخطاب السياسي وتضييق الكثير من مساحات الفضاء السيبراني المفتوح.	إحداث خلل متعمد في أداء أدوات ومعدات النسيج الشبكاتي وملحقاته.
طبيعة الأدوات والموارد المستخدمة	أدوات وموارد بسط السلطان السيبراني			
	داخل فضاء الفيض السيبراني		خارج فضاء الفيض السيبراني	
	أهداف ليّنة	أهداف صلبة	أهداف ليّنة	أهداف صلبة
موارد بشرية.	أنشطة مراقبة متنوعة يمارسها أفراد ومجاميع من جيش إيران السيبراني، فصائل رقمية لدى الباسيج، قراصنة مستأجرين، قراصنة متطوّعين.	ممارسة هجمات بواسطة قراصنة معلومات وفصائل رقمية حكومية، أو تناهض المعارضة.	وزارات ومؤسسات حكومية تعنى بمسائل إرشادية ودعوية ونشر خطاب الثورة الإسلامية الإيرانية.	مؤسسة الشرطة السيبرانية *FATA* التي تلاحق أصحاب الخطاب المعارض على الإنترنيت ومواقع التواصل الاجتماعي.
نظم معلومات.	استخدام محركات بحث وتطبيقات وطنية لمنصات التواصل الاجتماعي، ونظم	تبني مشروع شبكة الإنترنيت الإيرانية لحصر النشاط السيبراني داخل مضيفات الخدمة	توجيهات المجلس الأعلى لالفضاء السيبراني. الدور الذي يمارسه إعلام الثورة الإسلامية من جميع قطاعات الدولة.	الدور الذي تمارسه وزارة تقنية المعلومات والاتصالات والشركات التي تعمل معها.

طبيعة الأدوات والموارد المستخدمة	مواضع أهداف السلطان السيبراني			
	داخل فضاء الفيض السيبراني		خارج فضاء الفيض السيبراني	
	أهداف ليّنة	أهداف صلبة	أهداف ليّنة	أهداف صلبة
	تشغيل إيرانية صرفه. برامج التقطير السيبراني للمحتوى والجدران النارية.	الوطنية وعزل الفضاء السيبراني الإيراني عن الفضاء السيبراني العولمي.		

المصدر: من إعداد الباحث من خلال مراجعة أنموذج ناي وإجراء تعديلات جوهرية على مادته ومحاولة مطابقته على المشهد الإيراني.

ويبدو واضحاً من هيكلة الجدول أن دخيلة الفضاء السيبراني في إيران بدأ يتعرّض الى هجمات مكثفة توزعت على أهداف لّينة، وأخرى صلبة، وأن إيران قد حرصت على التعامل مع هذين المحورين بسلسلة إجراءات يمكن الوقوف على هويتها من فقرة الموارد البشرية التي تنتظم في هيكليات مؤسسية حكومية وأخرى فردية، على التوازي مع توظيف نظم معلومات وأدوات شبكاتية، حرصت على أن تكون مصنعة محلياً لضمان عدم اختراقها نتيجة التعاون والتنسيق بين الخصوم والجهات المصنعة.

أما المجال الفيزيائي الذي يقع خارج حدود فضائها السيبراني، فقد تبنت سياسة الارتقاء بالوعي الوطني لمواجهة آثار القوى الناعمة التي يستخدمها الخصوم مع ممارسة حربها الناعمة التي تعبر عن أهداف الثورة الإسلامية وغاياتها وقيمها. وبدأت بالوقت ذاته في ممارسة سلسلة من عمليات عزل منظومات *SCADA* عن الفضاء العولمي وحصره في فضاء محلي حصين، مع تفعيل دور الشرطة السيبرانية المحلية لمتابعة موارد الجرائم السيبرانية المحلية وكف شريحة واسعة من المستخدمين والقراصنة المحليين من ممارسة مخالفات تتعارض مع خطاطة الثورة الإسلامية الأمنية أو العقدية.

ونشب عن تكاتف أكثر من وزارة، ومؤسسة حكومية تقنية، أو أمنية، أو عسكرية، مع سعيها الى إذكاء روح المواطنة وصبغتها الوطنية التي تحنّ الى التراث الفارسي، من جهة، والرغبة بالتضحية من اجل المنظومة العقدية الشيعية، والولاء المطلق للإمام، من جهة أخرى بروز نمط فريد من السلطان السيبراني الذي تكاملت خيوط نسيجه من تكاتف هذه الجهات مجتمعة في ظل القفزات التقنية التي حققتها إيران في مضمار تقنية المعلومات والاتصالات، وتناسل أجيال أكاديمية متخصصة بهذه العلوم، في ظل عقد شراكات متينة مع دول تناوئ خصومها (كوريا الشمالية، روسيا والصين) الأمر الذي أنتج خليطاً سحرياً لدعم تنامي سلطانها السيبراني، وتحقيقها لقفزات تقنية، غير مسبوقة، رغم الحصار الذي فرض عليها، وعدم توفر فرصة كافية لصحوتها من آثاره العميقة، أو بدو نتائج استثمارها لنتائج التوافق النووي الجديد مع الغرب.

لقد أسهمت هذه الأمور مجتمعة في تعاظم السلطان السيبراني الإيراني على مستوى المنطقة، وبدأت طلائع قراصنة مؤسساتها العسكرية، والأمنية، والتقنية، والأكاديمية، بطرق البوابات والمنافذ السيبرانية للكثير من الأهداف في النسيج الشبكاتي بالولايات المتحدة، ودول أوربية، ودول خليجية، وأخرى بالمنطقة لتعلن قدرتها على بسط سلطانها ضمن

مساحة واسعة من فضاء الفيض السيبراني، سواء كانت لديها الرغبة بإحداث تأثير يتسم بصبغة عسكرية، أو أمنية، او يريد النيل من أهداف اقتصادية، أو صناعية، ومكنتها، بالوقت ذاته، على تحقيق غاياتها، في إحداث أضرار مؤثرة في الفضاءات المتخيّلة لخصومها الذين تفوقوا عليها على صعيد تقنيات وأدوات المواجهة على أرض الواقع الصلبة.

3. 1. مأسسة القرصنة السيبرانية وتشكيل السطوة السيبرانية الايرانية:

أجبرت النجاحات التي حققها قراصنة المعلومات الإيرانيين، وتطوير مهاراتهم على صعيد تجاوز العقبات التي رسخها النظام للحيلولة دون انتقالهم بحرية بين مواقع الويب، وتنامي قدراتهم في شن هجمات على مواقع محلية، وأخرى تقيم خارج حدود الفضاء السيبراني الإيراني، لإثبات جدارتهم، واختبار قدراتهم، الحرس الثوري الإيراني ومؤسسات أخرى مثل الباسيج على التفكير والتخطيط لتشكيل نواة لقوة ردع رقمية تستثمر هذه الطاقات، وتحاول إعادة توجيه مساراتها بحيث تسهم في دعم خطاب النظام، ودرء آثار الحرب الناعمة التي تتوجه بخطابها المعارض الى أعماق بعيدة في الفضاء السيبراني الإيراني، ليتلقفها المواطن الإيراني الذي أتقن صنعة القرصنة.

وأسهمت نظم المراقبة السيبرانية، والجهد الاستخباري المكثّف الذي تمارسه المؤسسات الأمنية الإيرانية في الكشف عن هوية الكثير من صفوة قراصنة المعلومات، الذين نشطوا في فضاء الفيض السيبراني، وباتت لهم بصمات واضحة في منتديات القرصنة المحلية والعالمية، فاستطاعت بعد سلسلة من المراجعات تجنيد عدد كبير منهم، واستثمار خبراتهم ومهاراتهم في تشكيل فصائل ووحدات رقمية، تدربت على أيدي هؤلاء القراصنة، وتعمل بإشراف وتوجيه مباشر من هؤلاء الصفوة، ومن خلال خطاطة تجزيئية، تقسّم تفاصيل الأنشطة، الى أنشطة ثانوية لا تكاد توحي للقراصنة أنفسهم طبيعة الأبعاد الاستراتيجية لممارساتهم الفردية، أو الجمعية عند شن هجمة على موقع، أو استهداف كيان رقمي، مع التوجه نحو صبغ هذه الأنشطة بصبغة قومية، في بعض الأحيان، أو صبغة عقدية تستثمر فيها ولاءات القراصنة العقدية، وحرصهم الشديد على الدفاع عن التراث العريق لبلادهم.

من أجل هذا اضطر النظام الإيراني على تشكيل خطاطة جديدة للتعامل مع القرصنة السيبرانية، خالفت الى حد كبير التوجه العولمي نحو تحديد هوية القرصان السيبراني (شان خلافاتها المستمرة بصدد مسائل أخرى تخص تفاصيل ملف برنامجنا النووي، وتطوير قدرات صواريخها البالستية، وحضورها السياسي والعسكري على ساحة أكثر من بلد من بلدان المنطقة، ونهج التفريق بين المقاومة والإرهاب، ومسائل أخرى).

فإذا كان التعريف التقليدي لقرصان المعلومات يحدد هويته باستخدام أدوات سبر مواطن الضعف والفجوات السيبرانية تمهيداً لمباشرة سلسلة من التأثيرات المزعجة أو الضارة بدءاً باختراق المواقع، أو إحداث خلل فيها، أو تشويش محتوى صفحاتها، أو التصعيد باتجاه شن هجمة لإيقاف الموقع أو تدميره، او إحداث أضرار مادية في الكيان السيبراني، أو المنظومات والبنى التحتية التي تستمد موارد أنشطتها بواسطة أدواته والخدمات التي توفرها لتسهيل عملية الإدارة ورقمنة أنشطتها المختلفة. فإنه يمكننا القول أن هناك إجماع عولمي على أن هناك فيصل يفرق بين الناشط السيبراني الذي يصدع بخطاب مناهض لنظام الحكم ومؤسساته المختلفة، ويدعو الى إصلاحات وتحسين الخدمات وضمان حرية التعبير عن الرأي، والقرصان السيبراني الذي يحاول التطفل على حمى ومجالات لا صلة له بها.

وهناك بالوقت ذاته ثمة تراتبية تحكم مختلف أشكال ممارسات القرصنة السيبرانية فتجعلها تتنقل بين قرصنة بيضاء تمارس تحت مظلة القانون للكشف عن حضور الفجوات الأمنية لغرض المسارعة في سدها ودرء تسلل المتطفلين والمجرمين من خلالها، تتجه نحو قرصنة رمادية تختلط بها الممارسة المشروعة مع غايات غير مشروعة، قبل أن تتحول الى قرصنة سوداء تعد ممارسة جرمية لا تختلف القوانين والتشريعات في تجريم أصحابها مع وجود اختلافات طفيفة في مستويات تجريمها بين هذا البلد وذاك.

وقد جعل النظام الإيراني خطاطة ثورته الإسلامية، وخطابه السياسي فيصلاً للتميز بين الممارسات المشروعة وغير المشروعة في الفضاء السيبراني الإيراني، والفضاء العولمي على حد سواء. فألحق جميع الممارسات التي لا تتفق مع خطاطته وخطابه السياسي، ومهما كان مستوى اختلافها، بدائرة الممارسات غير المشروعة، وعدّها نمط من أنماط القرصنة السيبرانية التي تلاحقها هيئة حظر المواقع لكي تخنق خطابها السياسي أو العقدي أو الثقافي، أو جعلها فريسة سهلة بين يدي أفراد شرطة فضاء إيران السيبراني تحكم قبضتها على أصحابها قبل أن تودع مرتكبيها في أقفاص الجرائم التي يعاقب عليها قانون الجريمة السيبرانية في إيران.

أما جميع أشكال ممارسات القرصنة السيبرانية، وبطيفها المتدرج من الرمادي نحو الأسود القاتم، فيعد بنظرها ممارسة مشروعة ما دامت تروم نشر خطابها العقدي والسياسي، أو تدرأ حضور الخطاب المعارض، بجميع أشكال ممارساتها السيبرانية. وأضحت الحروب اللينة ميداناً يسمح للنظام والجهات المتحالفة معه بشنّ مختلف أشكال الهجمات السيبرانية على المواقع التي تطرح خطابها المناهض، ومهما كانت طبيعة المحتوى والخطاب المطروح.

من أجل هذا تحوّل استعمال تطبيقات منصات التواصل الاجتماعي، بمنشوراته على موقع *Facebook*، والتغريدات السيبرانية على موقع *Twitter*، ونشر مقاطع فيديوية على موقع *YouTube*، ونشر الصور على موقع *Instagram*، (بنظر النظام) الى ممارسة قرصنة معلوماتية تقع في دائرة الأفعال الجرمية. كما أن جميع الخطابات التي تنادي بها المعارضة السلمية لمباشرة إصلاحات على أرض الواقع في إيران، أو الإفصاح عن معارضة خطاطة سياسية، أو المطالبة بالتخفيف من غلواء التشدد فعلاً يندرج في قائمة القرصنة والممارسات المخالفة للقانون.

من أجل هذا أدرجت على قائمة مهام الفصائل السيبرانية الدفاعية وقوة الردع الهجومية داخل حدود فضاء إيران شنّ هجمات، أو تتبع آثار حضور المعارضة، والحرص على تقطير مادة المحتوى، وملاحقة الناشطين السيبرانيين ومحاولة زجهم في زنزانة القضاء.

فتوسعت دائرة مأسسة القرصنة السيبرانية في البلاد، بعد أن روجع المفهوم داخل حدود البلاد، فأصبحت خطاطة القرصنة تتقبل ممارسات القرصنة التي تدرأ الهجمات عن المواقع الإيرانية، أو تجهض المعارضة التي تروم خلخلة الاستقرار بالبلاد، أو تنحو الى مهاجمة أهدافاً رقمية لبلدان تناهض برامج التنمية وتطوير قدرات البلاد في مجال التقنية النووية أو الدفاعية، وتعدها ممارسات مشروعة يرعاها النظام، ويحتضن أفرادها، ويوفر لهم موارد مالية مغرية. بالمقابل أضحت بحسب وجهة نظر النظام كل من ممارسات تجاوز الحظر المفروض على المواقع، أو بث الخطاب المناهض في تطبيقات منصات التواصل الاجتماعي قرصنة غير مشروعة يعاقب عليها القانون، وتلاحق أصحابها قوات شرطة الالفضاء السيبرانيي *FATA*.

من أجل هذا يمكننا القول إن محاولة النظام الإيراني إحداث تغيير جوهري في خطاطة القرصنة السيبرانية، ومأسسة أنشطة قراصنتها المحليين يعد السبب الأساس لتشكيل الحشد الكبير من الفصائل والميليشيات السيبرانية في إيران، وبشكل غير مسبوق، ولا نكاد نجد له تجربة مقابلة في دول أخرى. كما أن انبساط خطاب التشيع في أكثر من دولة بالمنطقة قد أسهم بتشكيل أكثر من بؤرة رقمية من قراصنة المعلومات المحليين الذين حرص النظام الإيراني على احتضانهم بالدعم والرعاية، ووظف سلطانه السياسي والعسكري والاقتصادي لإنتاج بؤر رقمية مؤثرة في المنطقة تروّج خطابه، وتمدّ سلطانه السيبراني على مساحة واسعة ومؤثرة بشكل لافت. وذلك بعد أن نجحت جميع التشكيلات السيبرانية بالتنسيق فيما بينها، لتوفر حصيلة عملياتها الاستخبارية، ونتائج هجماتها على المواقع المعادية أمام جميع فئات الفصائل والميليشيات السيبرانية لكي تستثمر في الإعداد والتخطيط للهجمات الجديدة على أعداء النظام، كما توفر بالوقت ذاته معلومات خصبة يمكن للجهات الأمنية أو القضائية أن تستثمرها لإحكام سيطرة النظام على فضاء الفيض السيبراني في عموم إيران.

4. خطاطة الاستراتيجية الإيرانية لحروب الفضاء السيبراني:

اختمرت مفردات الخطاطة الإيرانية لحروب الفضاء السيبراني وتكاملت سماتها البنيوية بعد أن تعايش الإيرانيون (بمختلف المواقع التي يحتلونها في معمارية بنيتها السياسية والأمنية، والعسكرية) على الحضور في فضاء رقمي مفتوح وخال من الحواجز قبل أن تبرز سياسات الحظر والكف بعد أكثر من عقد من الزمان.

لقد مرّت الخطاطة بسلسلة من التحوّلات فرضتها الظروف الاستثنائية التي عصفت بالبلاد والتي رافقت دخول خدمة الإنترنيت، مع وجود تراتبية فريدة في إدارة دفتها، يصاحبه تكاثر لافت في عديد مؤسساتها العقدية، والسياسية، والأمنية، وتباين مدارات اهتماماتها، ومقادير السلطة التي يمكن أن تمارسه كلا منها بصناعة القرارات الحاسمة في إيران الثورة الإسلامية.

من أجل هذا فقد نضجت عناصر هذه الخطاطة، وتطوّرت بنيتها المؤسسية، بعد أن مرّت باستحالات متدرجة فرضتها المتغيرات التي استنبتت في تربة إيران، وأثبتت، رغم التناقضات العميقة المقيمة في نسيجها، وتنافر بعض عناصرها، قدرتها على ترسيخ حضور لإعصار رقمي لافت في فضاء المنازعة والمواجهة السيبرانية الإقليمي والعولمي، وباتت تمتلك قدرات استثنائية شغلت مراكز البحوث في أوربا، والولايات المتحدة ووجهت دفة اهتماماتهم نحو دراسة تركيبتها المتفردة، مع السعي الحثيث الى تحديد كيفية مواجهة النمو المطّرد في شدة الإعصار التي بدأت تتنامى قوته ،بشكل لافت.

4. 1. مبررات ولادة الاستراتيجية السيبرانية ـ الإيرانية:

عند بداية دخول خدمة الإنترنيت الى إيران، ولج الالفضاء السيبرانيي عبر البوابات الأكاديمية، فكان حضوره إيذاناً بولوج المؤسسة العلمية والأكاديمية الإيرانية الى مجال سيدفع بعجلة التقدم في البلاد الى آفاق جديدة. وبعد الانفتاح التدريجي للفضاء الى مجالات جديدة في البلاد برز الهاجس الأخلاقي وتسللت مجسات الفتن المناوئة لخطاطة الثورة الإسلامية، ومبادئها الأخلاقية.

واستمر السجال بين دعاة إدخال الفضاء في ميادين ترقى بثقافة المستخدم الإيراني، وتعمّق اطلاعه على ما يحدث في الفضاء العلمي، وبين أنصار الحوزات العلمية، والملتحقين بالحرس الثوري وأنصاره الذين عدوا الفضاء الجديد تهديداً

عقدياً وامنياً بالقوت ذاته. بيد أن نوعاً من جسور المصالحة والثقة قد توثقت مع المؤسسات العقدية والحوزوية بعد أن استخدمت الأدوات السيبرانية وفضاءها المفتوح في نشر خطاب الثورة الإسلامية الى أماكن متباعدة، مع إنشاء محتوى رقمي رصين للمذهب الجعفري خلال بسط سلطانه على مساحات واسعة وبمدة قصيرة.

بيد ان هذه الهدنة المؤقتة، لم تدم طويلاً بعد نشوب الثورة الناعمة ـ الخضراء وامتداد تأثيرها على عموم الفضاء السياسي الإيراني عام 2009، وأعلنت الخصوم، وعلى رأسها الولايات المتحدة الأمريكية دعمها للحراك السيبراني، وسخرت خدمات داعمة لتطبيقات منصات التواصل الاجتماعي، وأوشكت الثورة الإسلامية أن تهدد بقوة في عقر دارها، الأمر الذي حتّم على النظام الإيراني الالتحاق بالتيار الذي تتزعمه مؤسسة الحرس الثوري والمحافظين والمتشددين من المؤسسات العقدية فعمدت الى استحداث عدد إضافي من المؤسسات (داخل حدود الدولة وخارجها) لضمان امن البلاد من التهديدات التي كانت مؤثرة خلال الحملة الانتخابية ولكفّ تهديدات أخرى قد تبرز الى الساحة السياسية والأمنية بالبلاد في المستقبل القريب.

لقد انتقل فضاء الفيض السيبراني الى ساحة الهواجس الاستراتيجية، بعد أن كان مستوطناً في مجالات أكاديمية، ومقارناً لممارسات اجتماعية بعيدة عن موارد قلق الحكومة ومؤسساتها العقدية والأمنية.

وقد تكللت الجهود بولادة المجلس الأعلى لالفضاء السيبراني الإيراني، عام 2012، وبهيئة يرأسها روحاني وثلّة من الوزراء، ونخبة من الشخصيات التي يرشحها القائد الأعلى للثورة، وممثلين من المؤسسات الحيوية، فبدأت معالم الاستراتيجية الوطنية، تتضح يوماً بعد يوم في ظل قيادة موحدة تلمّ شتات المراكز والمؤسسات المتكاثرة (التي توجّه مساراتها مراكز قوى وصنّاع قرار لا حصر لهم) التزمت بقراراتها المركزية التي أثبتت نجاعتها خلال مدة قصيرة، باعتراف مراكز بحوث أمريكية وأخرى إسرائيلية تعنى بمراجعة السياسات والاستراتيجيات السيبرانية على صعيد الفضاء السيبراني العولمي (*Siboni&Kronenfeld,2012*).

4. 2. السمات الفريدة للاستراتيجية الإيرانية السيبرانية:

يكاد أن يتفق جميع المتخصصين بدراسة تفاصيل الاستراتيجية السيبرانية لإيران على خصوصيتها واتصافها بجملة من المميزات الفريدة نتيجة لعوامل استنبت بعضها من أعماق التربة الإيرانية، التي تلتصق بجزيئاتها الصبغة التراثية والعقدية، شديدة الأثر، وعوامل أخرى فرضتها المواجهة المستعرة مع خصومها سواء الذين تفاقمت خصومتهم نتيجة لبرنامجها النووي المقلق، على التوازي مع برامج صواريخها البالستية، أو نتيجة لتعاظم سلطانها وتمدد مجسات تدخلها السافر في شؤون الدول الخليجية، ودول أخرى بالمنطقة، على التوازي مع تسعير النزاع الشيعي ـ السني في عموم العالم الإسلامي والتزامها بموقف الراعي والمدافع العنيد عن أنصار آل البيت حيثما وجدوا.

وقد أسهمت في تشكيل خصائص وأهداف استراتيجيتها السيبرانية، وأنتجت من هذا الخليط المعقد، استراتيجية أشد تعقيداً نتيجة للتشعبات المتعددة لخيوطها، وترابطاتها مع نسيج معقد من الهيكلة التنظيمية، التي غابت عنها سمة المركزية نتيجة لتعدد الكيانات العقدية، والسياسية، والعسكرية، مع التلاحم غير المسبوق بين هذه المؤسسات، وبين شريحة واسعة من الشعب، ورغم التناقض البيّن الذي يباعد فيما بينها، ببعض الأحيان، لحد المعاداة والمناهضة السافرة للنظام، ولأهداف الثورة الإسلامية، أو ممارسات كياناتها العسكرية والأمنية. هذه التناقض العجيب، في تلاحم

مكوناته وتنافرها بالوقت ذاته، أسهم في تشكيل هذه الاستراتيجية، وجعلها في أحيان كثيرة، عصية على الفهم، ويصعب التعامل معها وفق استراتيجيات الخصوم التي لم تألف التعامل مع خصوم من هذا النمط المحيّر!.

وقد أضافت نتائج دراسة الحالة التي قام بها الباحث كونيل (لاقتراح سبل ردع نزعة ممارسة إيران لسلسة من الهجمات والتهديدات السيبرانية ضد أهداف أمريكية مهمة) سمات أخرى للاستراتيجية السيبرانية الإيرانية، لعل أهمها (*Connell,2014*):

- ✓ وجود تباين واضح بين مفهوم الأنشطة الهجومية في الفضاء السيبراني، لدى الإيرانيين، وعدم انطباقها مع المفهوم لدى خصومها. ذلك لأن القيادة الإيرانية ترى أن تبني النهج الهجومي ـ السيبراني هو نتيجة حتمية لدرء آثار الحرب الناعمة التي تستهدف خطاطة الثورة الإسلامية، وتحاول تشويش الرأي العام للشعب الإيراني، مع تأجيج الفتن بالبلاد، الأمر الذي يشكّل تهديداً خطيراً يستوجب ممارسة هجمات رقمية، بينما لا ترقى تهديدات القوة الناعمة لدى بقية دول العالم الى مستوى يستحق ممارسة هجمات ذات طابع تأثير مؤثر وخطير كما هو الحال مع نهج إيران السيبراني في التعامل معها.
- ✓ تعدد الجهات التي تشارك في صناعة القرارات الاستراتيجية التي تخص حماية بيضة الثورة الإسلامية، سواء على المستوى العقدي (حيث تمارس المؤسسات الحوزوية الدور الأهم)، وأمن الثورة الإسلامية وحماية مكاسبها (حيث يمارس الحرس الثوري الإيراني هذه المهمة ويهيمن على جميع تفاصيلها)، وحماية أمن البلاد (حيث يمارس الجيش ممثلاً بفصائل جيش إيران السيبراني، وفصائل مؤسسة الباسيج السيبرانية وجهات أخرى عملية إدارة هذه المهام)، بالإضافة الى فصائل رقمية تتعدد ولاءاتها الى هذه الجهة أو تلك. الأمر الذي يجعل من الاستراتيجية متعددة المستويات، ومتباينة الأهداف، وتتنازع على ممارسة أنشطتها أكثر من جهة، تتباين مواقفها إزاء التهديدات والهجمات السيبرانية، مما يجعل عملية التنبؤ بنتائجها غير ممكناً، أو يحرّك النشاط نحو اتجاهات غير متوقعة.
- ✓ توظيف مجموعة من الوكلاء السيبرانيين، الذي يمثلون طيفاً واسعاً من قراصنة المعلومات/ من داخل إيران (مؤسسات، ومجاميع، وأفراد)، ومن خارجها (مجاميع وميليشيات) ومن دول متعددة، سواء كانوا مرتزقة، أو من المتطوعين المناصرين لنهجها، أو المتحالفين ضد خصومها. ويشكل هذا النهج عقبة حقيقية إزاء أي محاولة لتتبع مسارات الهجمات، او التنبؤ بتفاصيل استراتيجيتها، إذا علمنا أن إيران تديم مراجعة مستويات اعتمادها على هذه الفرق، في ظل أولويات تتعلق بجملة من المتغيرات الداخلية والخارجية، الأمر الذي يمنح الاستراتيجية غموضاً أكبر.

من أجل هذا يمكننا القول أن الاستراتيجية الإيرانية (على صعيد فضاء الفيض السيبراني) قد اتسمت بجملة من الخصائص الفريدة، شأن تركيبة صناعة القرارات السياسية فيها، حيث تتشابك الخيوط التي تمسك بتلابيبها جهات متعددة، وتتميز كل منها بنهج يختص بتركيبتها المؤسسية، ينصبغ بالخطاطة العقدية، والسياسية، او الأمنية التي يتصف بها أعضاؤها، وتتأرجح بمعادلة توازن القوى الداخلية، وتنازع السلطات، غير المعلن، والذي يدير دفته الرئيسة القائد الأعلى للثورة.

4. 3. محاولة لوصف الاستراتيجية السيبرانية ـ الإيرانية:

أسهمت الانتفاضة السيبرانية (أثناء الحملة الانتخابية لعام 2009، والهجمات المؤثرة التي توجهت آثارها نحو إحداث تأثيرات ضارة في البرنامج النووي الإيراني) في إحداث صحوة رقمية لدى النظام الإيراني وأجبرته على إعادة التفكير بسياساته السابقة، والتوجه بقوة نحو تبني خطط انفجارية لتطوير آلاتها الدفاعية، والهجومية، مع تطوير هيكلة مؤسساتها التي تعنى بإدارة جميع تفاصيل الحضور السيبراني الإيراني في الفضاء السيبراني.

وعدّت الحكومة الإيرانية مسألة الأمن السيبراني الوطني من المسائل المهمة على صعيد صيانة الأمن القومي للبلاد، وأعلن القائد الأعلى للثورة عن توجيهه بتشكيل المجلس الأعلى لالفضاء السيبراني الإدارة العليا ودعي رئيس الجمهورية الى الالتحاق به، مع مجموعة شخصيات من كابينته الوزارية، بالإضافة الى مجموعة من الأعضاء المنتخبين، والمراقبين من جميع القطاعات للإسراع بإعداد الأطر العامة والتفصيلية لضمان أمن وحصانة الفضاء السيبراني، مع إعادة تشكيل قيادة لإدارة فصائل القوى العسكرية الأمنية (التي تسهر على حماية الفضاء السيبراني الوطني) مع مد جسور التعاون مع المؤسسات الأكاديمية والبحثية الوطنية لبناء القدرات وتطوير المهارات(*Siboni&Kronenfeld,2012*).

وقد خصصت الحكومة بضعة مليارات من الدولارات لتنفيذ وتطوير مجموعة من المشاريع ذات الاهتمام بمسائل الأمن والسلطان السيبراني للبلاد (*Katz,2011*)، فحققت انتفاضة بعموم إيران وظّفت فيها العداء المستفحل للولايات المتحدة وحلفائها بالمنطقة، وألبست ما تتعرض له من تهديدات لمعادة ذات طابع عقدي يعادي المذهب الجعفري، وهي من المسائل التي تجمع جميع المتخاصمين في إيران وتعد القاسم الأكثر تأثيراً في ممارسة تصعيد الشعور الجمعي الإيراني إزاء التهديدات التي تمسّ الهوية والانتماء لبلاد فارس، والولاء العقدي للمذهب ومسألة الإمامة (*Siboni&Kronenfeld,2014*).

بصورة عامة، توحّدت رؤية النظام الإيراني في تشكيل الخطوط العامة للاستراتيجية السيبرانية بعد أن انتظمت جميع مؤسساتها تحت راية المجلس الأعلى لالفضاء السيبراني في عام 2012. بيد أن هذا التوحد في الاستراتيجية لا ينفي وجود سياسات متعددة تتبناها كل مؤسسة من هذه المؤسسات بحسب تأثير انتماءاتها وولاءاتها.

بصورة عامة تتألف هذه الاستراتيجية من ثلاثة محاور[197]، محور يعنى بالدفاع عن الحياض السيبرانية للفضاء الوطني الإيراني من هجمات متكررة يمارسها خصوم البلاد، وعلى رأسهم الولايات المتحدة الأمريكية وحلفائها، وخصوم إقليميون، وآخرون تدفعهم خلافات عقدية. ومحور هجومي يحاول الرد على الهجمات بممارسات هجومية بوصفه نهجاً يقلل من التأثير المتزايد للهجمات على الأهداف الاستراتيجية والحيوية بالبلاد.

[197] . ذهب معظم المتخصصين بدراسة استراتيجية الفضاء السيبراني الإيراني الى تبني أنموذج بمحورين لوصف عناصر هذه الاستراتيجية، واحتواء المحور الثالث ضمن المحور الدفاعي، أو جعل المحور الثالث للتأثير على الهيمنة الأمريكية في الفضاء السيبراني العولمي. بيد أن تحليلنا لسياسات الحوكمة السيبرانية ـ الإيرانية مع مراجعة حجم التخصيصات الاستثمارية التي خصصتها الحكومة لتلبية احتياجات الكفاية الأمنية لهذا المحور يجعل من إفراده خطوة ضرورية، نظراً للأهمية التي توليها الحكومة بحماية أمن فضائه (*Siboni&Kronenfeld,2012*).

أما المحور الثالث فيعنى بترسيخ أمن الفضاء الداخلي من خلال محاربة جرائم المعلومات، وحظر التصرفات المناهضة لنهج الثورة الإسلامية، ومنافحة آثار الثورة الناعمة التي باتت تشكل تهديداً يهدد تماسك المجتمع الإيراني، والتفافه حول رموز البلاد ومرجعياتها[198].

المحور الأول: محور إحكام أمن الفضاء السيبراني المحلي:

إن الموقف الذي يتخذه النظام الإيراني تجاه انفتاح المستخدم الإيراني على فضاء الإنترنيت، وبلوغ تخوم المناطق المحظورة وفق الخطاطة العقدية والأمنية للثورة الإسلامية يكاد يرقى الى مستوى المواجهات مع خصوم البلاد، الأمر الذي فرض على الحكومة التفكير في صياغة استراتيجية محلية للتعامل مع التجاوزات المستمرة لعدة فئات من المجتمع الإيراني، ومشاركة بعضهم في تصعيد الثورة الناعمة المناهضة لمبادئ الثورة وقيمها.

ويعزى هذا الأمر الى حرص المواطن الإيراني على استخدام الإنترنيت[199] وحرصه على ولوج أماكن يشدّه إليها فضوله المعرفي، ورغبته العميقة بالتخلص من سلاسل القيود المتعددة التي فرضها النظام على بوابات متنفسه بهذا الفضاء العولمي.

ويكمن التحدي الذي يشخص أمام الإدارة الحكومية في التعامل مع هذا الملف في ميل المستخدم الإيراني الى استخدام الشبكات الافتراضية الخاصة *VPN* لتجاوز عقبة حظر المواقع وتوظيف آليات التقطير السيبراني على محتوى صفحات الويب.

لقد توجهت الحكومة الإيرانية (من خلال تشكيلات مؤسساتها العسكرية والأمنية) وبالتنسيق مع حلفائها من قراصنة المعلومات المحليين نحو ممارسة سلسلة من الهجمات على الكيانات السيبرانية التي تلتحق بها المعارضة بقصد إضعاف شوكة المعارضين وقطع جسور الدعم المحتمل من الجهات التي تؤجج لهيب الثورة الناعمة ـ المعارضة في إيران، من جهة، ولدرء المخاطر الناجمة عن هجمات قراصنة ينتمون الى جهات متعددة من المناوئين، داخل حدود البلاد وخارجها، لإحداث خلخلة في عمل شبكة الإنترنيت بالبلاد، أو التلصص على مواقع حكومية مهمة، وإحداث خلل في مضيفات الخدمة المحلية، ومهاجمة مواقع القيادات العليا الإيرانية، ونشر خطابات معارضة في تطبيقات منصات التواصل الاجتماعي.

وقد انتظمت جميع الممارسات الحكومية للتعامل مع هذا الملف وفق الاستراتيجية التي تبناها وسعى الى تنفيذها المجلس الأعلى لالفضاء السيبراني، وبالتنسيق مع الجهات الحكومية ذات الصلة بهذا الملف، والتي تضمنت بذل جهود حثيثة لتحقيق ما يأتي (*Siboni&Kronenfeld,2012*):

---

[198] . لخص خبراء معهد دراسات الأمن الوطني الإسرائيلي *INSS* توجهات الإدارة الإيرانية بالتعامل مع صياغة مفردات استراتيجيتها في فضاء الفيض السيبراني *Modus Operandi In Cyberspace* بثلاث خطوات جوهرية (*Siboni& Kronenfeld, 2012*):

الأولى: توجيه عناية خاصة نحو تطوير القدرات الدفاعية ـ السيبرانية لكف واحتواء الهجمات والتهديدات السيبرانية التي تمارسها الكيانات السياسية للدول المعادية لإيران، والكيانات السيبرانية (مجاميع، وفرق وقراصنة معلومات) يعادون خطاطة الثورة الإسلامية وسياساتها بالمنطقة.

الثانية: تطوير قدرات عملياتية لكياناتها ومؤسساتها السيبرانية لممارسة هجمات معلوماتية ضد خصومها ضمن سياسة المعاملة بالمثل.

الثالثة: توفير حصانة أمنية ـ رقمية لدى إيران لمواجهة التفوّق الأمريكي في إدارة دفة الفضاء السيبراني وسطوتها في تهديد الغير عبر قنوات الفضاء السيبراني.

[199] . أطلق الكثير من الباحثين على الشعب الإيراني لقب **الشعب السيبراني** *Cyber Nation* .

أولاً: الجانب الهجومي من الاستراتيجية:

- ممارسة سلسلة من الهجمات على مواقع الجهات المعارضة لكف عملها وإحداث خلل في مادة خطابها السيبراني[200].
- دعم قراصنة المعلومات المنتمين الى الحرس الثوري الإيراني، والباسيج، والجيش السيبراني الإيراني في مهاجمة تطبيقات لمنصات متعددة بقصد إيقافها عن العمل.
- توجيه شرطة إيران السيبراني *FATA* بتتبع مصادر الخروقات السيبرانية وإلقاء القبض على المستخدمين الذين تورطوا بممارستها وإيقاع عقوبات صارمة بحقهم[201].

ثانياً: الجانب الدفاعي / الوقائي من الاستراتيجية:

وضعت الإدارة الحكومية (قبل إنشاء المجلس الأعلى لالفضاء السيبراني، واستمرت بعد أن تبوأ مركز المخطط الأساسي لصياغة استراتيجيات إيران السيبرانية) نصب عينيها سياسة تألفت من ثلاثة خطوات أساسية لإحكام أمن الفضاء السيبراني المحلي في البلاد. فقد حرصت على:

- ✓ الهيمنة على إدارة قنوات فضاء الفيض السيبراني والتحكم بمساراته، وإحكام المراقبة على مضيفات الخدمة، والشركات التي تطرح الخدمة للمستخدمين وفي ظل تعليمات ورقابة أمنية صارمة[202].
- ✓ استخدام نظم مراقبة صارمة وذكية لمتابعة أدق تفاصيل المحتوى السيبراني المسافر في تطبيقات التواصل الاجتماعي، أو المطروح على صفحات مواقع الويب، وخدمات البريد الإلكتروني لجعل المواطن الإيراني عرضة للمراقبة الدائمة في جميع الممارسات التي يمارسها أثناء حضوره بالفضاء السيبراني.
- ✓ تضييق قنوات الفيض السيبراني لشبكة الإنترنيت وذلك عن طريق تقليص سرعة الخدمة[203] لمنع المستخدمين من تحميل أو رفع الملفات المرئية من / الى مواقع مثل: *YouTube*، أو الوصول الى مواقع ويب تتعارض مضامين الخطاب المطروح في صفحاتها مع خطاب الثورة الإسلامية في إيران.

---

[200] . اختراق موقع شركة امن المواقع الألمانية *DigiNotar* وذلك للحصول على معلومات تدعم جيش ايران السيبراني في الحصول على شهادات *Google* مزيفة بقصد استخدامها للتجسس على الاتصالات الخاصة بين المستخدمين الإيرانيين التي توظف تطبيقات *Google* (*Schwarz,2013*).

[201] . أولى الاعلام الغربي اهتماماً بالغاً بالممارسات العنيفة لشرطة الفضاء السيبراني بإيران *FATA* لفرض هيمنتها على الفضاء السيبراني بالبلاد، عندما شاع خبر تصفية المدوّن الإيراني ستار بهشتي عام 2012 في إحدى السجون القريبة من طهران بعد أن وقع بقبضة الشرطة السيبرانية، مما جعل الاتحاد الأوربي يعلن فرض حصاراً عليه (*Siboni&Kronenfeld,2014*).

[202] . مورست سلسلة من هجمات رفض الخدمة *DOS* على تطبيق منصة التغريد السيبراني *Twitter* وذلك لكف محاولات بث التغريدات التي نظمت الانتفاضة الخضراء خلال الحملة الانتخابية الرئاسية عام 2009 ونشر خطابهم المعارض، والافصاح عن التعامل العنيف مع المعارضين، بعيداً عن أطواق الرقابة والحظر السيبراني (*Schwarz,2013*).

[203] . تصل سرعة الإنترنيت في الدخول الى بعض المواقع المحظورة الى أقل من 10% من السرعة المتوفرة للمواطن الإيراني، علماً أن الخدمة في إيران هي الأكثر بطءً على صعيد المنطقة.

- ✓ حظر برمجيات التناقل الصوتي عبر الإنترنيت *Voice-over-IP* (مثل: تطبيقات *Skype, Google Talk*) وفرضت عقوبات قضائية صارمة على استخدام برمجيات القفز فوق نظم الحظر والمراقبة الحكومية مثل: *VPN, TOR* والتي تموه هوية المستخدم وتغيب عنونة حضوره السيبراني.

- ✓ تقليص نسبة حضور الفضاء السيبراني العولمي في فضاء الفيض السيبراني بإيران عن طريق الإسراع بعملية التحول نحو شبكة الإنترنيت الوطنية التي تتسم بمضيفات خدمة محلية، وتطبيقات إيرانية تنطق باللغة الفارسية، وتلتزم بخطاب الثورة الإسلامية وثقافتها وثوابتها. في خطوة نحو عزل الفضاء السيبراني المحلي عن الفضاء السيبراني العولمي وتوفير خدمة الإنترنيت الحلال بدلاً من الخدمة الغربية المشحونة بالفتن، والضلالات، والتهديدات المبطنة للثورة الإسلامية وثقافتها.

- ✓ إنشاء المزيد من الهيئات الرقابية والتي تمارس نشاطها في الفضاء السيبراني الإيراني، لممارسة الضغط على المستخدمين، وحظر المواقع، وإحكام السيطرة على محتوى صفحات الويب المحلية، والسعي الى حظر المواقع التي تطرح محتوى رقمي يخالف ثقافة الوثرة الإسلامية. وتعد هيئة تشخيص المحتوى المواقع غير المرخصة من هذه الهيئات، والتي تعكف على تشخيص هوية المواقع المخالفة، وغير المرخصة، ثم تقوم بالتنسيق مع الجهات المعنية لإدراج هذه المواقع على قائمة المواقع المحظورة والتي لا يسمح للمستخدم الإيراني بالوصول اليها. وتقوم شرطة الفضاء السيبراني بعملية تتبع ممارسات المستخدمين الإيرانيين المخالفة، والتلصص على خطابهم التواصلي عبر تطبيقات شبكات التواصل الاجتماعي، بالإضافة الى مهمتها الأساسية في محاربة الجرائم السيبرانية. وهناك ايضاً الوحدة المدنية في جهاز الباسيج، والتي تقوم ببث خطاب دعائي يناهض المعارضة ويدعم النظام (*Schwarz,2013*).

ولازالت الإدارة الحكومية الإيرانية، وبالتنسيق مع طيف واسع من مؤسساتها التخطيطية، والتنفيذية مستمرة في سعيها لتهيئة موارد بشرية محلية داعمة لهذا المحور من محاور استراتيجيتها، وتوفير أرضية تقنية صلبة على صعيد أدوات وتطبيقات أدوات المعلومات والاتصالات لإكمال مشروع شبكة الإنترنيت الوطنية، وطرح تطبيقات بديلة لتطبيقات منصات التواصل الاجتماعي، وآلات بحث، ومستعرضات تمتلك إمكانيات وقدرات تجذب المستخدم الإيراني بعيداً عن مصادر وموارد الإنترنيت التي باتت تشكل تهديداً متزايداً ومصدراً للقلق الدائم، وبوابة مشرعة لتهديدات تستنزف موارد مالية، ومعلوماتية من موارد البلاد.

المحور الثاني: محور مدافعة ودرء التهديدات الخارجية:

وتستهدف السياسات الإيرانية في هذا المحور توفير حصانة أمنية، ومؤثرة لمدافعة ودرء المخاطر الناجمة عن التهديدات والهجمات السيبرانية التي يباشرها خصومها (بالدرجة الأولى) وغيرهم على البنية التحتية للمعلومات والاتصالات بالبلاد، والبيانات الحساسة، والمشاريع والبرامج النووية الطموحة، أو تقويض أركان الحضور السيبراني الإيراني على الإنترنيت، بجميع مظاهره، السياسية، والعقدية، والاقتصادية، والاجتماعية.

ولضمان غايات هذا المحور وأهدافه، توجهت الإدارة الحكومية نحو إنشاء نظام دفاعي متعدد المستويات يجمع بين مجموعة أنشطة تشمل: مراقبة تخوم الفضاء السيبراني الإيراني، مع توفير أدوات رقمية محلية (قدر الإمكان) قادرة على حفظ أمنه، ومحاولة عزل الأجزاء المهمة عن الفضاء العولمي وربطها بالفضاء المحلي لشبكة الإنترنيت الوطنية،

أو باعتماد مضيفات خدمة تستقر على الرقعة الجغرافية للبلاد[204]، وتشكيل قوة رادعة تمتلك مهارات رصينة لإدارة المنظومة الوطنية الدفاعية، مع إطلاق سلسلة من برامج التوعية للارتقاء بمستوى الوعي الأمني ـ السيبراني كجزء من عملية المدافعة ودرء الأخطار.

ويمارس المجلس الأعلى لالفضاء السيبراني دور المخطط الاستراتيجي وصاحب الكلمة الطولى في تحديد تفاصيل عناصر استراتيجية هذا المحور، وانتخاب أفضل الآليات التي تتوافق مع حجم التهديدات القائمة، ووفرة الموارد المادية والبشرية المحلية. وتقوم مؤسسات الدولة بتنفيذ هذه السياسات والخطط بدءاً بوزارة تقنية المعلومات والاتصالات، ومنظمة الدفاع السلبي، وجيش إيران السيبراني، والفصائل السيبرانية المرتبطة بمؤسسة الباسيج، وشرطة الفضاء السيبراني *FATA*، والمجلس الأعلى للثورة الثقافية بتنفيذ سياسته على أرض الواقع، وفي المجال السيبراني لالفضاء السيبراني (*Siboni&Kronenfeld,2014*).

وقد دعمت الإدارة الحكومية مراكز البحوث والتطوير التقني، والشركات الصغيرة التي تعنى بتصنيع أدوات المعلومات والاتصالات، وبالتنسيق مع وزارة تقنية المعلومات والاتصالات، ومراكز بحوثها، ووفرت لهم التسهيلات لتنمية صناعات وطنية لأدوات المعلومات والاتصالات التي تستخدم في قطاع الأمن السيبراني (تطبيقات برمجية لكف الفايروسات والديدان الضارة، جدران ناري، ومعدات متنوعة) وذلك في سعيها المستمر للتقليل من اعتمادها على أدوات دفاعية، تنتج في بلدان تناصبها العداء، او خارجها، مما قد يشكل استخدامها فرصة لاستغلال ثغرات أمنية (غير منظورة) لمباشرة التهديدات أو الهجمات على بنيتها التحتية السيبرانية والاتصالية[205].

ولعل من الإنجازات التقنية المهمة في مضمار ترسيخ أمن المعلومات بالبلاد ، ما أعلنت عنه وكالة الأنباء الإيرانية *ISNA*، عن بدء الإدارة السيبرانية في إيران في استخدام نظام حماية أمنية متكاملة أطلق عليه اسم شاهباد. وسيقوم هذا النظام، بحسب تصريح مدير المشروع ـ محمد نادري، بإعداد مشهد رقمي متكامل لجميع تفاصيل الفيض السيبراني الوطني، والمتولد عن أنشطة محطات المستخدمين والمتحسسات السيبرانية. وستسهم هذه الصورة السيبرانية في توفير أرضية أمنية متينة تنذر النظام في حالة حصول أي تهديد او هجمة رقمية في البلاد. وسيقوم النظام بإعلام الجهات المسؤولة عن أمن الفضاء السيبراني ونسيجه الشبكاتي، لغرض اتخاذ إجراءات سريعة لدرء هذه التهديدات أو الهجمات، ومنعها من تحقيق غاياتها وتوجهاتها التخريبية (*Siboni&Kronenfeld,2014*).

---

[204] . باشرت الإدارة الحكومية الإيرانية بوضع الخطوط الأساسية لمشروع شبكة الإنترنيت الوطنية مع بدايات عام 2009 لضمان فصل الفضاء السيبراني الإيراني عن الفضاء العولمي وترسيخ حضوره من خلال مضيفات خدمة *Internet Providers* في داخل إيران، وإنشاء بيئة برمجية وطنية تدعمها محركات بحث ومستعرضات، وتطبيقات إيرانية تناظر التطبيقات المنتشرة بكثافة في الفضاء العولمي. وبوشر بالتشغيل التجريبي لأجزاء محدودة من هذه الشبكة بعد مرور ثلاث سنوات من بدء المشروع، ولا زال العمل مستمراً مع التأخير المستمر في توقيتات عملية العزل نتيجة للحصار المفروض على إيران، بالإضافة الى عدم كفاية الخبرات والموارد المحلية (المادية والبشرية) مع تزايد حجم الطلب، وتطور التقنية السيبرانية على الصعيد العالمي.

وقد لاحظ الباحثون في إحدى مراكز البحوث الأمنية بالولايات المتحدة، عند تحليل العقد السيبرانية في الفضاء السيبراني الإيراني، قيام الإدارات السيبرانية بالبلاد بتثبيت عنوانين لكل حاسب *IP Address* بدلاً من العنوان الأحادي، في إشارة الى وصف موقع الحاسب على الشبكتين العالمية والمحلية (*Siboni& Kronenfeld,2014*).

[205] . أعلن في احتفال (خلال شهر كانون الأول 2013) حضره كل من وزير الدفاع الإيراني، الجنرال حسين دهقان، ومسؤول الدفاع المدني غلام ريزا جليلي، ومسؤولين من مؤسسات حكومية متعددة عن نجاح المؤسسات الإيرانية وكوادرها التقنية في إنتاج أكثر من 12 منتج لدعم الأمن السيبراني الوطني، شملت: هاتف محمول آمن ضد عمليات التنصت الالكتروني، وإطلاق نظام تشغيل وطني آمن بعيداً عن الحاجة الى استخدام نظم التشغيل التي تنتج بالولايات المتحدة الأمريكية، وتطوير برمجيات مكافحة الفايروسات والديدان الضارة، إضافة الى إنشاء جدران نارية، وتصنيع معدات رقمية . شبكاتية متنوعة(*FARS News Agency, Dec.,14th,2013*).

ولم تغب عن بال الإدارة الحكومية الإيرانية فرصة استثمار التنافس الأمني المستعر بين روسيا الاتحادية، أو كوريا الشمالية، أو الصين، وتوتر بعض مفاصل علاقاتهم مع الولايات المتحدة وبعض حليفاتها، في عقد اتفاقيات مشتركة للتعاون التقني لتزيد إيران بمعدات تقنية، وتدريب مواردها البشرية، في خطوة لسد الفجوة في مجال الخبرات وتباين مستوى المعرفة مع خصومها عند مواجهة التهديدات المستمرة، ودرء المخاطر المحتملة التي قد تنجم عنها (*Siboni&Kronenfeld,2014*).

كذلك وجهت اهتمامها نحو مسألة بناء القدرات، فوجهت رعايتها نحو تطوير المهارات من خلال برامج تدريبية رصينة، واختبار إمكانات مواردها على مواجهة الهجمات السيبرانية المحتملة من خلال إجراء سلسلة تمارين عسكرية تدريبية لمحاكاة مجال المواجهة والمدافعة في فضاء افتراضي، وعلى مستوى الوحدات المدنية والعسكرية وبإشراف مباشر من قبل الحرس الثوري الإيراني.

وقد أجريت التمارين على التوازي مع مناورات عسكرية لأكثر من فصيل من فصائل الجيش الإيراني، وبحضور فاضل للمؤسسات الدفاعية المدنية، نذكر منها المناورة التي قام بها الحرس الثوري الإيراني في مضيق هرمز عند نهاية عام 2012 حيث مورست سلسلة هجمات معلوماتية على منظومة حواسب الأسطول الإيراني المشارك بالمناورة، واختبار قدرات فصائل جيش إيران السيبراني على استعادة البيانات وإزالة تأثير الدودة الخبيثة التي أقحمت في النظام. وقد نجح فريق أمن المعلومات الذي يعمل في الأسطول في اكتشاف الهجمة والسيطرة على الوضع وتجاوز تأثيراتها (*Siboni&Kronenfeld,2014*).

واجري تمرين أمني آخر في شهر أكتوبر من عام 2013، بيد انه كان تحت مظلة المناورة الدفاعية العامة لمؤسسة الدفاع السلبي، وقد اشترك في هذا التمرين عدد كبير من المؤسسات الحكومية الإيرانية ـ الحساسة، بقصد اختبار قدراتها الأمنية السيبرانية. وشمل التمرين: المنشآت النووية، وشبكة مترو طهران، وهيئة الإذاعة الإيرانية، وموانئ ومطارات إيرانية، والبنك المركزي الإيراني، ومجهزي خدمة الهواتف المحمول بعموم البلاد.

كان هذا التمرين محاولة لإعادة تقييم الكفاية الأمنية للمؤسسات الإيرانية الحساسة بعيد الهجمات التي مارستها دودة *Stuxnet* وكذلك *Flame* على منشآتها النووية ولإعادة الثقة بمنظومة الدفاع السيبراني الإيراني بعد الاختراقات المتتالية التي نالت منظوماتها السيبرانية خلال عام 2012 (*Siboni&Kronenfeld,2014*).

وكذلك يمكن أن تعد هذه المناورة إشارة الى تهديد مبطن للولايات المتحدة الأمريكية وإسرائيل (اللتان اشتركتا في التخطيط وتنفيذ هذه الهجمات) بقرب نشوب هجمات إيرانية على أهداف استراتيجية لدى هذين الخصمين، وأن فصائل الدفاع السيبراني الإيراني أضحت قادرة على صد الهجوم المضاد الذي سيمارس للانتقام من الآثار المدمرة للهجمات السيبرانية الإيرانية والتي باتت وشيكة.

ومن جهة أخرى أعلنت وكالة أخبار فارس عن النجاح الكبير الذي حققته هذه المناورة السيبرانية العملاقة، وأثبتت حصانة الفضاء السيبراني الإيراني، وقدرة فصائل الدفاع السيبراني في مؤسسة الدفاع السلبي، وفصائل جيش إيران السيبراني على درء المخاطر المحتملة من هجمات أعداء إيران وخصومها بالمنطقة. بيد أن المراجعة للقرارات التي صدرت لتقييم أداء أنشطة المناورة، تظهر للمتخصصين وجود ثغرة في الحماية السيبرانية للمؤسسات النووية الإيرانية،

ذلك لأن الجهة المشرفة على المناورة قد أوصت بإنشاء مركز منفصل لعمليات الدفاع السيبراني في منشآت مشروع نطنز النووي.

المحور الثالث: محور الهجوم والردع السيبراني:

يشكّل الفضاء السيبراني مجالاً جديداً للمنازلة والمدافعة بين الخصوم تغيب عن ساحته المتخيّلة معايير توزان القوى التقليدية بعد أن ترك المجال مفتوحاً أمام استخدام آليات المواجهة غير المتساوقة *Asymmetric Warfare* التي أتاحت لأن تتدافع وتتخاصم مجاميع صغيرة مع كيانات عملاقة، وتحدث تأثيراً معنوياً لا يتناسب مع توازن القوى المتحاربة في مجالات المواجهة في سوح المنازعة التقليدية.

وقد استثمرت إيران هذه الميزة لكي ترجّح كفة تنازعها ومخاصمتها المستديمة مع الولايات المتحدة وحلفائها بالمنطقة، فوجهت جهوداً كبيرة لتطوير قدراتها في هذا المجال للتقليل من حجم الفجوة التقنية التي تفصلها عن خصومها على صعيد التقنية العسكرية، ولإضافة قدرات مضافة تسهم في التأثير على الجهات التي تهاجم المواقع الإيرانية، وتصرف انتباهها باتجاه الدفاع عن أهداف تستقر في فضائها الوطني.

بيد أن الهجمة الشرسة لفايروس *Stuxnet* والتي امتدت بين عامي 2009 و2010، (وأحدثت تدميراً في منشآت إنتاج اليورانيوم المنشط بلغت نسبته حوالي 20%) قد أسهمت الى حد كبير في إحداث صحوة إيرانية، ونهضة رقمية سريعة بعد أن عمدت الإدارة الحكومية في ولاية روحاني بزيادة كبيرة في حجم التخصيصات المالية المخصصة للارتقاء بقدرات إيران الدفاعية والهجومية، على صعيد الموارد المادية والبشرية على حد سواء، بحيث عدّ خبراء المعهد الإسرائيلي لدراسات الأمن السيبراني *INSS* أن التهديدات التي ستصاحب هذه النهضة السيبرانية ستكون أشد خطورة من التهديد النووي المحتمل عن تطور قدراتها التقنية في هذا المضمار (*INSS,2015*).

استعذبت الإدارة الحكومية الإيرانية مبدأ الحرب غير المتماثلة، وتعاملت معها بوصفها فرصة ثمينة يمكن أن تفسح امامها مجالاً مفتوحاً للتأثير على خصومها دون القلق رغم عدم رجاحة كفة قدراتها الهجومية قبالة القوة الغاشمة التي تمتلكها الولايات المتحدة وأنصارها في المنطقة، ويعد بالوقت ذاته عنصراً مضافاً الى ممارسات أخرى تطرق بواسطتها على الأبواب الخلفية لخصومها.

لقد نبه التهديد الذي مورس بواسطة الفايروس *Stuxnet* على المنشآت النووية في إيران، مع إحداثه لأضرار بالغة في أجهزة الطرد المركزي، الى حقيقة توفر فرصة أمام الذراع السيبراني الإيراني الفتي لزيادة صلابة عوده، والبدء بممارسة تهديدات مماثلة على البنى التحتية الأمريكية (سواء محطات توليد طاقة كهربائية، أو محطات نووية، أو منظومات النقل المواصلات، وغيرها من المنشآت التي تعتمد في عملها بكثافة على شبكات المعلومات والاتصالات المنفتحة على فضاء الإنترنيت)، في تحقيق غايتين، (الأولى) ترجيح كفة تفوقها العسكري في المنطقة، مع الارتقاء بتراتبية حضورها العولمي، و(الثانية) التلويح بهذه القدرات أمام الخصوم لكف ممارساتهم الهجومية المتكررة على البنية التحتية الإيرانية، بجميع مفاصلها الحيوية، وتحقيق نوع من التوازن المقبول على صعيد المواجهة ـ مع الآخر في فضاء النزاع السيبراني (*Schwarz,2013*).

وقد أثمرت الجهود الحثيثة للإدارة الحكومية في تجميع ولملمة قدرات مواردها البشرية ـ العارفة والمنبثة في الوزارات، والحرس الثوري الإيراني، ومؤسسة الباسيج، ومراكز البحوث التقنية، والمؤسسات الجامعية، مع توفير تخصيصات

مالية كبيرة في دفع العجلة السيبرانية بالبلاد، وترسيخ القدرات السيبرانية الهجومية بحيث أصبحت إيران في مكانة متقدمة على صعيد السطوة السيبرانية بالمنطقة، وعموم الفضاء العولمي.

صنّف مجلس الأطلنطي (مركز أبحاث أمريكي متخصص في مسائل أمن المعلومات) السلطان السيبراني لإيران ضمن المرتبة الثالثة *Third Tier* في التراتبية العولمية للسلطان السيبراني، حيث تستقر بالمرتبة الأولى *First Tier* كل من الولايات المتحدة الأمريكية، وروسيا، والمملكة المتحدة، بينما تستقر في المرتبة الثانية *Third Tier* كل من الصين وكوريا الشمالية

وذهب التقرير الذي أعده هذا المركز الى أنه رغم وجود إيران في المرتبة الثالثة فإن هذا الأمر لا يقل من تأثيراتها المحتملة على خصومها الذين يستقرون بالمرتبة الأولى، بسبب تكاثر وجود الثغرات الأمنية في النسيج الشبكاتي وتطبيقاته التي توفر لديها فرصة لإحداث تأثيرات غير متوقعة، بيد أن هذه التأثيرات لا زالت متراجعة عن مستوى التأثيرات ذات البعد الاستراتيجي على خصومها (*Slavin&Healy,2013*).

بيد أن خبراء معهد دراسات الأمن الوطني الإسرائيلي *INSS* لا يتفقون مع هذا الرأي، بعد أن أكدوا (في دراستهم المعمقة لتحديد ملامح التطورات الحاصلة في قدرات الحروب السيبرانية بإيران خلال السنتين 2013-2014) على امتلاكها لموقع مميز على ساحة المسرح العولمي لحروب المعلومات، كما أن التطورات الحاصلة في قدراتها خلال البعد الزمني لدراستهم مع تطور القدرات الهجومية بشكل لافت، مع تطوّر آلياتها، وانتقاء أهدافها بعناية لافتة للانتباه (*Siboni&Kronenfeld,2014*).

إن المراجعة المتأنية، وتحليل الوقائع ذات الصلة بممارسة الأنشطة الهجومية في فضاء المنازعة السيبرانية الذي تستوطن فيه موارد وأدوات السلطان السيبراني الإيراني، يمكن أن تبوح لنا ببعض الخصائص الجوهرية لهذا المحور، والتي يمكن أن نلخصها بما يأتي:

- ✓ استخدام جميع الوسائل والتقنيات المتوفرة، في الفضاء السيبراني لممارسة التهديدات والهجمات السيبرانية، بجميع مستوياتها، بقصد إشغال الخصوم وإحداث خلخلة (حتى ولو كانت محدودة)، على التوازي مع تصاعد توجهاتها نحو تطوير قدراتها الهجومية والمؤثرة. ويلاحظ أن جل الهجمات التي قامت بها كوادر المؤسسات الحكومية الإيرانية، وجيش إيران السيبراني، والميليشيات السيبرانية المحلية، في الفسحة الزمنية التي سبقت عام 2012 قد وظفت آليات رفض الخدمة *DDoS*، وقرصنة نظم أسماء النطاقات الخاصة بالمواقع *DNS Hijackings* والتي تعد من التقنيات البدائية ومحدودة التأثير على صعيد الهجمات السيبرانية (*Connell,2014*).
- ✓ بناء مجموعة من التشكيلات المرتبطة، بقطاعات مختلفة، تقوم بممارسة الهجمات السيبرانية، وتمثل الذراع السيبراني ـ العسكري للبلاد، فهناك وحدات رقمية تعمل تحت مظلة وزارة الدفاع الإيرانية، وهناك جيش إيران السيبراني الذي يشرف عليه الحرس الثوري الإيراني، وهناك وحدات تعمل مع مؤسسة الباسيج، والتي تتكاتف جميعاً في تطوير قدراتها ومهاراتها، مع إدامة تنسيق الهجمات ضد أعداء البلاد.

- ✓ تشجيع ورعاية أنشطة القرصنة السيبرانية لدى طيف واسع من الكوادر المحلية التي تمتلك مهارات معلوماتية في مجال الاختراق، والتنقير عن الثغرات السيبرانية، والأمن السيبراني مع إضفاء سمة الدفاع عن الوطن، وحماية الخطاطة العقدية للمؤسسات الحوزوية، وتبني شعارات تؤجج الحس الوطني لكي ينضم الى جيشها حجم كبير من المتطوعين الذين يحرصون على درء المخاطر عن بلاد فارس ويحمي أرثها العريق من التهديدات المحتملة[206].

- ✓ تشجيع تأليف ميليشيات رقمية تنضبط بأطر تنظيمية تشرف عليها مؤسسات مثل: الحرس الثوري الإيراني، والباسيج، وجهات أخرى تسير بهدي التيار الحوزوي المتشدد بحيث تدعم الذراع السيبراني المؤسسي وتنفتح على مساحة واسعة في استهداف أهداف متنوعة لدى الجهات المناوئة في فضاء المنطقة، والفضاء العولمي.

- ✓ مد جسور الثقة، وترسيخ أوجه التعاون مع قراصنة المعلومات المنتشرين في الفضاء العولمي، والسعي الى تجنيدهم من خلال عقد تحالفات معهم، على أساس التقارب في الأهداف السياسية، أو العقدية، وفي ظل توفير دعم مالي، أو توحيد الأهداف تجاه جهات محددة لزيادة سلطانها السيبراني في ممارسة الهجمات السيبرانية ضد الغير.

- ✓ تمتين وتوسيع نطاق التحالفات والشراكات، المعلنة منها وغير المعلنة مع الخصوم التقليديين لعدوها، الشيطان الأكبر (الولايات المتحدة الأمريكية)، وتوحيد الجهود في ممارسة الهجمات التكافلية والمنسقة بمساعدة كل من: روسيا، وكوريا الشمالية، والصين.

- ✓ توسيع رقعة البؤر السيبرانية الداعمة للنظام الإيراني، في الرقع الجغرافية لتحالفاتها العقدية والسياسية، من خلال توفير الدعم التقني والمالي واللوجستي لكل من: جيس سوريا السيبراني، والكوادر السيبرانية لحزب الله في لبنان، والذراع السيبراني لحركة حماس في قطاع غزة، والذراع السيبراني في اليمن. وذلك لإدامة سلطانها السيبراني في منطقة الشرق الأوسط، وضغطها المستمر على خصومها بالمنطقة، مثل: إسرائيل، والسعودية، ودول خليجية أخرى، والتأثير على خصمها العنيد الولايات المتحدة بالوقت ذاته.

لقد أثبت هذه الاستراتيجية نجاحها على أرض الواقع، نتيجة لسمة التنوّع وتعدد المحاور التي توجهت نحوها مساراتها، وتكاثر عديد الجهات التي تساهم في تنفيذ أهدافها على أرض الواقع، وتنوّع انتماءاتهم، وتباين أماكن استيطانهم السيبراني. وقد برزت معالم نجاحها وانعكاساتها المباشرة على نمو السلطان السيبراني الإيراني في الفضاء السيبراني العولمي، والممتد على مساحة جغرافية واسعة، بعد أن وثقت مجموعة كبيرة من الهجمات التي تأكد قيام المؤسسات السيبرانية الإيرانية، والقراصنة الإيرانيون، وحلفائهم بمباشرة ضد أهداف حيوية تستقر في النسيج الشبكاتي لخصومهم بالمنطقة في عقر دار بلدان أوربية، وبالولايات المتحدة الأمريكية. والتي أكدت حصول طفرة نوعية في

---

[206] . أظهرت الدراسة التي قام بها الباحث *Connell* استمرار النظام الإيراني بعملية إعادة تقييم القدرات المتوفرة لدى قراصنة المعلومات المحليين والميليشيات السيبرانية العولمية، وبحسب طبيعة العلاقات ومتانتها التي تربطها بالمؤسسة الحكومية والقطاعات الأخرى. وذلك تمهيداً لصياغة مسارات التعاون معها في الفضاء السيبراني لمباشرة الهجمات ضد أهداف منتخبة (*Connell,2014*).

آلية الهجمات، وبروز مستوى متقدم من التعقيد التقني اللافت، وعمق التأثير على الأهداف المنتخبة، وتطاول البعد الزمني لتأثير الهجمات، وتخارج تأثيرها الى خارج حدود الفضاء المتخيل باتجاه أهداف مقيمة في نسيج البنى التحتية لقطاعات الطاقة والنقل، والخدمات المدنية، بعد أن نجت بالتوغل الى داخل حدود مؤسسات حكومية مهمة، ومؤسسات عسكرية تقيم في حلف الناتو، أو داخل حمى وزارة الدفاع الأمريكية (البنتاغون).

وإذا كانت الهجمات الإيرانية، في بداياتها غير قادرة على الولوج الى أعماق النسيج الشبكاتي لخصومها، واقتصرت تأثيراتها على إغراق المواقع بسلسلة طلبات تؤدي الى توقفها بصورة جزئية، أو ممارسة عملية تغيير مسارات الوصول الى مواقع الخصم باتجاه مواقع ملفقة تقوم بإنشائها الجهات الإيرانية المهاجمة وشحنها بمحتوى رقمي مناهض. لذا كانت تأثيراتها محدودة ويمكن تلافي تأثيراتها بسرعة، ودون حصول تخريب معنوي في العقد السيبرانية المستهدفة. إلا أن الهجمات التي بدأت بممارستها بعد عام 2012 قد اتسمت بخصائص مؤثرة بصورة لافتة، بعد أن أضحت أكثر نضوجاً، وأشد تأثيراً، ونخص بالذكر منها عملية "سيف العدالة القاطع على منظومة حواسب شركة أرامكو تسببت بضياع بيانات أكثر من 30 ألف حاسب بالشبكة التسويقية للشركة بواسطة فايروس ضار أطلق عليه فايروس شامون *Shamoon Virus* ثم امتد تأثيره الى شركات نفطية في قطر(*Connell,2014*). الأمر الذي اجبر وزير الدفاع الأمريكي السابق، بانيتا، على الاعتراف صراحة بأن الهجمات الإيرانية الأخيرة على شركة أرامكو السعودية، تعد سابقة خطيرة، وناقوس خطر ينبئ بتهديدات أشد خطورة قد تطال الولايات المتحدة وحلفاءها بالمنطقة العربية في وقت قريب من إيران (*Schwarz,2013*).

4. 4. التطورات الحاصلة على سياسة إيران في مجال الدفاع والردع السيبراني:

لعل من السمات المميزة، والتي تشكل تهديداً خطيراً لخصوم إيران، داخل حدود الفضاء الفيض السيبراني، حرص النظام الإيراني على تبني سياسة متعددة الأطراف، وتعتمد معمارية من نمط جديد في ممارسة سياستها في هذا الفضاء.

فعلى صعيد الكيانات المساهمة في ترجمة هذه الاستراتيجية الى ممارسات رقمية، بشقيها الدفاعي والهجومي، نلاحظ تعدد الكيانات السيبرانية التي تخطط وتنفّذ تفاصيل هذه الاستراتيجية، بين مؤسسات ترتبط مباشرة بالمؤسسة العسكرية الرسمية، وأخرى تنتمي الى مؤسسة الحرس الثوري الإيراني، على التوازي مع حضور مكثف لميليشيات رقمية تتوزع بين منظمة الباسيج، وفصائل كربلاء، ومجاميع القرصنة التي تتحالف مع هذه المؤسسات مجتمعة في تشكيل كيان افتراضي تصعب عملية الكشف عن جوهره، وهوية الكيانات الملتحقة به، وطبيعة العلاقة التي ترتبط بين كياناته، هو جيش فضاء إيران السيبراني. وبين كيانات رقمية لا تنتمي الى إيران بصورة مباشرة، ولكن تشترك معها بمناصبة العداء لنظم سياسية معادية لإيران، بعضها ينتمي الى كيانات سياسية متحالفة مع إيران، مثل نظام بشار الأسد في سوريا، وحزب الله في لبنان، وحركة حماس وفصائل فلسطينية أخرى في قطاع غزة، وحركة الحوثيين في اليمن. وأخرى تتألف من مجاميع قراصنة المعلومات الذين يعرضون خدماتهم لشنّ الهجمات ضد أي هدف مقابل مكاسب مادية، يوفرها النظام الإيراني لتمويل أنشطتهم بعد أن يضفي على مساراتها وانتخاب أهدافها ما يصبّ في زيادة مظاهر سلطانه السيبراني في فضاء الفيض السيبراني المفتوح، ولقرع أجراس تنبه خصومه على ضرورة إعادة مراجعة حساباتهم لأكثر من مرة قبل مباشرة أي هجمة ضد إيران، بعد أن بدت مطالع سطوتها السيبرانية خلال السنوات الخمس الأخيرة.

ويزيد من خطورة الأمر حرص إيران، وقدرتها على إخفاء أي بصمة من بصمات حضورها في سيل الهجمات التي تشن على الولايات المتحدة، ودول غربية، ودول عربية تقع في دائرة خصومة إيران ومناهضة سياساتها وممارساتها في منطقة الشرق الأوسط، وبقع جغرافية أخرى في العالم بحيث لم تكتمل الأدلة أو تترسخ لرفع أصبع الاتهام نحو إيران وإلصاق تهمة ممارسة الهجمات للنظام الإيراني، في فضاء متخيل، وحضور افتراضي لكياناتها، مع توفر أكثر من فرصة لتغييب آثار بزوغ الهجمات أو منتهاها بشكل ينمّ عن سياسة ذكية، وتنفيذ محكم لا تشوبه شائبة، أو تحضر فيه فجوة تكاد تفصح عن هوية الفاعل، أو المنسّق الذي يدير هذا السيل المتلاطم من الهجمات السيبرانية المتكاثرة.

وقد اكدت الدراسة التي قام بها باحثون من مركز المعهد الأمريكي للتهديدات الحرجة (*Kagan&Stiansen,2015*) أن إيران تمتلك أكثر من فرصة لتغييب بصمات حضورها من مواقع بزوغ أو ممارسة هذه الهجمات عن طريق استخدام وكلاء رقميين، سواء كانوا افراداً أو شركات، تستقر داخل إيران أو في العالم الغربي، يسعون للحصول على خدمات استضافة لمواقعهم وحضور كياناتهم السيبرانية في الولايات المتحدة، أو كندا، أو بريطانيا، أو ألمانيا، ودول أخرى، وتوفر لهم التغطية المالية لهذه الأنشطة، مع توفير مختلف أشكال لدعم لكي تباشر التهديدات والهجمات من مواقعهم، بعيداً عن حدود فضاء إيران السيبراني، فتنأى بها عن إلصاق التهم، أو إدراج ملف سلطانها السيبراني على مناضد الأمم المتحدة شأن ملف برنامجها النووي.

ولزيادة حصانة النسيج الشبكاتي الإيراني، وترسيخ مناعة بنيته التحتية قبالة الهجمات والتهديدات السيبرانية حرص النظام الإيراني على ممارسة عملية توزيع القدرات والمهارات المحلية في جميع طبقات معمارية البنيات المؤسسية لمعظم الوزارات، وبشقيها الدفاعي والهجومي. وسعى بالوقت ذاته، الى توطيد مستوى عال من التنسيق، والتعاون التقني، واللوجستي بين جميع هذه الكيانات المؤسسية لضمان تماسك خطاطة أمن المعلومات، واحتواء الثغرات الأمنية وتقليل المخاطر التي قد تنجم عنها الى الحدود الدنيا.

وأظهرت لنا عملية التنقير في العناصر الجديدة بسياسة إيرانية للدفاع والردع السيبراني أن النظام قد حرص على بناء كيان مؤسسي متين، متعدد الطبقات، ومتشعب الارتباطات، يمتد على مساحة واسعة من المهام التي تمارسها الوزارات المختلفة، ويحرص على أن يستثمر جميع الطاقات المتاحة لكي تصب حصيلتها في البوتقة التي قد خصصت لإنتاج التوليفة الخاصة بخطاطة امن المعلومات الإيراني، مع تطوير السلطان السيبراني الوطني.

وقد انتخبت الجهات التي ألحقت بالهيكلة المؤسسية المعقدة، التي كلفت بهذه المهمة لضمان تحقيق جملة من الأهداف الحيوية، منها:

- ✓ منح المجلس الأعلى لالفضاء السيبراني صلاحيات واسعة، بعد أن وطنت فيه نخبة من صنّاع القرار، مع توفير مرونة عالية في تسيير المهام بحيث تدعم التحرك السريع والرشيد تجاه التعامل مع التهديدات المحتملة، وتنفيذ سياسة البلاد وفق الخطط التي تبناها النظام.
- ✓ بناء قدرات وطنية متميزة في مجال أمن المعلومات والردع السيبراني من خلال اعتماد سلسلة من برامج التدريب للكوادر المتوسطة، وتطوير قدرات العاملين في مراكز البحث والتطوير، ومؤسسات التعليم العالي لضمان إنتاج كوادر متقدمة في هذا القطاع لها القدرة على الوقوف بوجه التهديدات والهجمات التي تتسم بتعقيد تقني لافت.

- ✓ الظفر بقفزة تقنية نوعية في مجال تصنيع عتاد المنظومات السيبرانية التي تستخدم لضمان أمن النسيج الشبكات، وأخرى يمكن استثمارها في تعزيز قوة الردع السيبراني للبلاد، من جهة، مع السعي الى إنتاج وتطوير منصات برمجية، ونظم تشغيل، وبرمجيات متخصصة لمكافحة والتقليل من آثار البرمجيات الخبيثة، ونشر برمجيات هجومية في الفضاء السيبراني للجهات التي تعادي النظام، من جهة أخرى.
- ✓ السعي الى الإعلان عن ممارسات الدفاع السيبراني ومؤسساته وإضفاء الشرعية على الدور الذي يمارسه النظام في درء المخاطر عن فضائه السيبراني، وتجنب الإعلان عن ممارسات الردع السيبراني، وربطه بقراصنة معلومات وناشطين من داخل البلاد أو خارجها، في محاولة لتغييب أية آثار قد تمنح خصومها فرصة توجيه أصابع الاتهام الى النظام في ممارسة مثل هذه التهديدات أو الهجمات السيبرانية على المواقع الحيوية في الولايات المتحدة، أو دول أوربية تناهض سياسته أو برنامجه النووي الصاعد.
- ✓ استثمار المهارات المتزايدة لقراصنة المعلومات في إيران، وإدارة دفة هذا النشاط الذي بات يؤرق المؤسسة الأمنية الإيرانية، من خلال عقد صفقات غير معلنة يمكن من خلالها كسب المزيد من الوكلاء السيبرانيين للعمل مع آلة النظام في الكشف عن الثغرات السيبرانية، وممارسة هجمات على أهداف منتخبة في الفضاء السيبراني لخصومه.
- ✓ بناء بؤر رقمية منتخبة في البقع الساخنة بمنطقة الشرق الأوسط، حيث يستعر الخلاف بين أنصار المعسكرين السني والشيعي وتأليف فصائل وميليشيات رقمية تنافح عن قضيتها من جهة، وتدرأ عن إيران المخاطر السيبرانية نتيجة لإشغال خصومها بمعالجة آثار الهجمات، من جهة أخرى. وقد توزعت هذه البؤر الرقيمة في كل من: لبنان بواسطة الفصائل السيبرانية لحزب الله، وفي سوريا من خلال جيش سورية الإلكتروني، وفي اليمن من خلال فصائل الحوثيين السيبرانية، بالإضافة الى بؤر أخرى لم تطفو آثار تهديداتها على السطح لغاية هذا التاريخ.

5. السجالات السيبرانية في الفضاء السيبراني الإيراني:

يزدحم الفضاء السيبراني الإيراني بسيل متنوع من النبضات السيبرانية التي توظف لممارسة طيف واسع من السجالات السيبرانية، التي لا تقل في شدتها، عما يدور من سجالات سياسية، وعقدية، في فضاء الواقع الإيراني، المشحون بنزاعات داخلية وإقليمية وأخرى دولية، منذ زمن بعيد.

وقد استثمرت الأطراف المتنازعة، مجتمعة، السمات الفريدة التي يتسم بها فضاء الفيض السيبراني لنقل جزء لا يستهان به من محصلة النزاعات والسجالات الى الفضاء المتخيل، لضمان تصعيد النزاع، وتمديد أذرع سلطانه الى مساحات محظورة لا يمكن بلوغها على أرض الواقع.

وبدأت مساحة السجال السيبراني تتطور يوماً بعد يوم، فأضيفت إليها جبهة داخلية تتقاسم النزاع فيها السلطة مع المعارضة السياسية والأثنية، ثم بزغت ساحة السجال مع خصوم إيران من الدول الكبرى، والدول الإقليمية، واقتصر النزاع في بداياته على حظر المواقع غير المرغوبة، ثم تحول باتجاه ممارسة تهديدات، لم تلبث أن تحولت الى هجمات بقصد إقحام رسائل تهديد، أو شعارات مناوئة. ثم تطور النزاع وتطورت أدواته بحيث تحول الى أداة ردع فاعلة

نجحت الولايات المتحدة وإسرائيل بتوظيفها في إحداث خلل كبير في البرنامج النووي الإيراني، ولم تتأخر إيران بالرد على هذه الهجمة بهجمات متتالية باتت تشكل تهديداً على منظومات تشغيل محطات الطاقة والسدود بالولايات المتحدة، وبلدان أوربية أخرى، وبلوغ مستودعات البيانات الاستراتيجية لدى الكثير من خصومها.

لقد تحول الفضاء السيبراني من ساحة نزاع إضافية، محدودة الاستخدام، وبوصفها عنصراً داعماً لساحة النزاع التقليدي، الى ساحة نزاع أصيلة لا يمكن الاستغناء عنها لتنفيذ استراتيجيات تتوافق مع القدرات المتاحة في مجتمع المعرفة والتواصل المفتوح.

5. 1. بزوغ ممارسة السجال السيبراني في الفضاء السيبراني الإيراني:

انتهجت إيران نهج الحرب غير المتساوقة *Asymmetrical Warfare* منذ بضعة عقود بقصد إحداث تأثيرات ضارة بخصومها للتقليل من حجم المخاطر المحتملة من مناوئتها ومناصبتها بالعداء، ولتعويض الفرق الكبير في موازين القوى نتيجة للتفوق التقني الذي تمتلكه الدول الكبرى.

وقد نجح هذا النهج في درء الكثير من المخاطر المحدقة بإيران نتيجة لنجاحها في إشغال القوى المناوئة في نزاعات إقليمية، أو درء تهديدات تمارسها كيانات متفرقة، هنا وهناك، تمولها بصورة مباشرة، أو غير مباشرة لإحداث تشويش متعمد في المشهد السياسي، أو الاجتماعي، أو الاقتصادي.

وقد برزت التهديدات والهجمات السيبرانية بوصفها خياراً إضافياً يمكن أن يستثمره النظام الإيراني لإحداث بلبلة رقمية في فضاء معلومات الدول المناهضة لخطاطته، وبكلف استثمارية منخفضة، وباستغلال سمة الانفتاح، وتغييب هوية الفاعلين في الفضاء المتخيّل.

لم تكن ممارسة هذا النهج، في بدايتها ذات بعد تأثيري ملموس، بعد أن انحصرت ممارساتها في مهاجمة مواقع، أو إيقاف خدمة المضيفات لبضعة ساعات، أو تشويش مادة خطاب مطروح على هذا الموقع، أو ذاك. بيد أن الطفرة التقنية التي واكبت ولادة جيل فايروس *Stuxnet* وما تناسل عنه من برمجيات خبيثة أضحت قادرة على إحداث تأثيرات ضارة في البنى التحتية لمنشآت توليد الطاقة، وإدارة قطاعات متعددة من مجتمع المعلومات الذي يرتكز بكثافة الى أدوات المعلومات والاتصالات، قد لفتت انتباه الإدارة الحكومية في إيران نحو الاستثمار بتنمية قدراتها الهجومية لممارسة النمط الجديد من الحروب المتماثلة التي أمست تأثيراتها أشد وطأة على الخصوم بحيث بدأت خاصية اللا تماثل تغيب تدريجياً عن ساحة المواجهة مع تقارب السلطان السيبراني لدى البلدان المتقدمة مع الدول النامية التي تحسن إدارة قدراتها في فضاء متخيّل، لم تعد موازين القوى في مجاله تشابه القواعد التي تسري على مجال موازين القوى التقليدية.

وقد عكف النظام الإيراني على بناء سلطانه السيبراني، من خلال تشكيل نواة مؤسسية لالفضاء السيبراني امتدت سلطتها على مجموعة واسعة من تشكيلات ووحدات الفضاء السيبراني التي حرص على نشرها على مساحة مؤسسية واسعة، شملت: القطاع الأكاديمي والمؤسسات البحثية بقصد استثمار خبرات الكوادر الجامعية المتقدمة والباحثين المتخصصين بتقنية المعلومات والاتصالات، وهندسة الالكترونيات، وامن المعلومات، والرياضيات والفيزياء، مع محاولة جذب الطلبة الملتحقين بالدراسات الأولية العليا، ممن يتمتعون بمهارات وقدرات متميزة لكي يلتحقوا بالعمل في

مركز بحوث إيران للاتصالات *Iran Telecommunications Research Center* أو يتوجهون نحو الالتحاق ببرامج تدريب توفرها مراكز تدريبية متخصصة تهيؤهم لكي يكونوا قراصنة معلومات متميزين في المستقبل. (*HP,2014,a*)

وقد سخّرت الصلاحيات الواسعة التي يتمتع بها تشكيل التعاون والتنسيق التقني في مكتب رئيس جمهورية إيران لدعم المشاريع المتميزة، وتسخير الإمكانيات المادية واللوجستية لترجمتها الى كيانات وقدرات رقيمة في الفضاء السيبراني الإيراني، يدعم استراتيجية النظام، ويعزز من حضور سلطانه السيبراني في الفضاء العولمي.

وقد استثمرت نتائج هذه الخطوات بحيث انعكست آثارها بجلاء على قدرات وسلطان الآلة الأمنية والعسكرية للنظام في الفضاء السيبراني. حيث شهدنا ولادة قيادة عمليات الدفاع في الفضاء السيبراني *Cyber Defense Command* التي ولدت في رحاب منظمة الدفاع السلبي بعد أن ربطت بالقيادة العامة للقوات المسلحة الإيرانية. وقد توسع نطاق نشاط هذا التشكيل بعد أن التحقت به ثلة من ممثلي مؤسسات وزارات: الدفاع، وتقنية المعلومات والاتصالات، والمخابرات، والصناعة. ولم يتخلف عن الالتحاق به ممثلين عن مراكز البحوث التقنية والأكاديمية، لكي تكتمل في دائرته القدرات التقنية والعسكرية والأمنية في سبيل إنتاج خطاطة رقمية إيرانية تحكم قبضتها على ملف الحصانة الأمنية للكيانات السيبرانية الإيرانية قبالة التهديدات القادمة من تخوم الفضاء السيبراني العولمي.

وعززت قدراتها الدفاعية بتأسيس وتفعيل الدور الذي بدأت بممارسته شرطة فضاء إيران السيبراني *FATA* الذي بدأ بملاحقة بذور الجريمة السيبرانية في إيران، ومكافحة موارد البيئة الحاضنة لها، مع تكليفه بحماية الفضاء السيبراني المحلي من ممارسات المعارضة والناشطين السيبرانيين الذين يعارضون النظام ويطرحون خطاباً مناهضاً لثقافته، كخطوة لاحقة لإجراءات هيئة مراقبة المواقع غير المرخصة.

ولم تستطع المؤسسات المتخصصة (بدراسة ملفات أمن المعلومات في الولايات المتحدة أو دول أوربا) إنكار الدور الكبير الذي مارسته مؤسسة الحرس الثوري الإيراني في تطوير آلة الدفاع والردع السيبراني الإيراني خلال عقدين من الزمان، ونجاحها في ترسيخ حضور خطاطتها وتعميق حضور صبغتها العسكرية المتشددة في مجال السلطان السيبراني للنظام الإيراني. (*HP,2014*)

وقد حرص النظام، وبجميع مفاصل مؤسساته عن إبعاد الأنظار عن ساحته بصدد ممارسة الهجمات السيبرانية ضد الكثير من بلدان المنطقة، وخصومها في الاتحاد الأوربي، وعدوها التقليدي الولايات المتحدة، نتيجة لتضييع الآثار، وتغييب البصمات من خلال التركيبة المؤسسية التي استمت بانبساطها على مساحة واسعة، مع المبالغة في تفريعات ارتباطاتها، بالإضافة الى مباشرتها في فضاء مفتوح، تغيب فيه الهوية، وتضمحل فيه بصمة الولاء والانتماءات.

وبذلك استطاع الحرس الثوري الإيراني توسيع دائرة حضوره السيبراني، وتطوير ممارساته، وزيادة قدرات قراصنته وتعميق الآثار التي تمارسها أدواتهم، فعكفت كوادره على إنتاج جيل جديد من البرمجيات الخبيثة، وإقحام شيفرات مؤذية في النسيج الشبكاتي للخصوم ونظمها السيبرانية بعيداً عن ايداعها في قفص الاتهام.

5. 2. موارد التهديدات والهجمات السيبرانية ـ الإيرانية:

أظهرت تحريات شبكة *Norse Intelligence Network* الاستخبارية (والتي كثفت جهودها خلال أكثر من عقد من الزمن لمراقبة ورصد أنشطة القرصنة السيبرانية التي تنشأ من العقد السيبرانية التي تستوطن الفضاء السيبراني الإيراني)

أن جلّ هذه الهجمات تتم برعاية مباشرة من قبل مؤسسات حكومية، أو مجاميع، أو أفراد يدينون بالولاء للثورة الإسلامية ويتلقون دعماً لوجستياً سخياً من مؤسسات عسكرية وأمنية. كما أفلحوا بالعثور على عقد معلوماتية تقيم خارج إيران وتمارس هجمات تصب في مصلحة النظام، الأمر الذي يؤكد على حضور فاعل لوكلاء رقميين نجحت إيران بتجنيدهم للعمل تحت مظلة برامج استراتيجيتها الأمنية ـ السيبرانية (*Kagan&Stiansen,2015*).

وقد أقدم فريق الدراسة على تقسيم موارد الهجمات السيبرانية التي مارستها الفصائل السيبرانية الإيرانية، وبمختلف انتماءاتها وتوجهاتها، وبصرف النظر عن هوية الهدف السيبراني الذي تحاول ممارسة الهجمة السيبرانية إزائه، الى ثلاثة أقسام أساسية (*Kagan&Stiansen,2015*):

- **القسم الأول:** هجمات متفرقة تنشأ عن حزمة واسعة من عناوين الإنترنيت *IP Addresses* التي توفرها مختلف فئات مضيفات الخدمة الإيرانية، لشريحة واسعة، ومتنوعة من المستخدمين الإيرانيين. وتؤشر مثل هذه الهجمات الى محاولات فردية لمستخدمين يحاولون ممارسة أنشطة قرصنة بدائية لا تمتلك تأثيراً ملموساً على الأهداف، أو قد لا تنجح ببلوغها، أو نشاطات قرصنة متفرقة يحاول من خلالها بعض قراصنة المعلومات الإيرانيين ترسيخ بصمتهم ضمن أنشطة مجتمع القراصنة المتنوع. وفي جميع هذه الحالات لا يشكل حضور هذه الفئة من المستخدمين أو قراصنة المعلومات، ولا ممارساتهم التهديدية أي أثر معنوي يستحق الذكر.
- **القسم الثاني:** هجمات تحتضن مواردها في مضيفات تعود الى مؤسسات حكومية إيرانية، مثل مؤسسة الحرس الثوري الإيراني، أو جامعات إيرانية، ومراكز بحوث تعنى بملف أمن المعلومات وتطوير تقنياته. بصورة عامة، تلعب مؤسسة الحرس الثوري الإيراني دوراً مهماً في التخطيط، واختيار الأهداف، وتنسيق المهام بين الجهات المشاركة في الحملات السيبرانية، بالإضافة الى توفيرها بنية تحتية متماسكة قادرة على احتضان الجهات وتوفير كافة المستلزمات التقنية واللوجستية اللازمة لضمان نجاحها.

وقد حرصت هذه المؤسسة على تغييب هذا الحضور عن الواجهة لدرء التهم التي قد توجه إليها من خصومها من داخل البلاد وخارجه، فغيّبت حضورها كلياً عن مواقع الويب المنتشرة على فضاء الإنترنيت بحيث لا يمكننا العثور على موقع يختص بها، رغم أن وزارة الدفاع الإيرانية، ومؤسسات عسكرية وأمنية أخرى تمتلك مواقعاً تختص بها وتعلن عن بعض نشاطاتها في فضاء الإنترنيت.

بالمقابل فقد أسست لحضورها المغيّب مجموعة من المواقع التي تختص بمؤسسات حكومية، أكاديمية واتصالية، وأخرى تعود الى مجاميع قراصنة معلومات إيرانيين، بات تشكّل نواة ولحمة بنيتها التحتية السيبرانية والاتصالية، وأضحت تمارس التهديدات والهجمات السيبرانية عوضاً عنها لضمان استبعادها عن مشهد الحروب السيبرانية المستعرة مع الولايات المتحدة وغيرها من الدول المناوئة للنظام الإيراني (*Kagan&Stiansen,2015*).

وتعد جامعة الإمام الحسين *Imam Hossein University (IHU)* مرتعاً خصباً لاستضافة مجموعة متنوعة من مواقع الويب، ومضيفات البريد الإلكتروني، ومواقع أخرى لتغطية أنشطة هذه الجامعة. لقد نجحت مجموعة الخبراء العاملين في *Norse Intelligence Network* الاستخبارية في تحديد عنون الإنترنيت التي توظفها هذه المؤسسة الأكاديمية لممارسة نشاطها السيبراني في فضاء الأنترنيت، ووجدت أن حزمة هذه العنونة كانت مسؤولة عن شن 13 هجمة معلوماتية خلال المدة بين يونيو 2014 ومارس 2015. كذلك شنّت 12 هجمة معلوماتية بين شهري مارس

ويونيو من عام 2013 تبين أنها قد صدرت عن مصرف *Sepah* وهو المصرف الذي يعمل تحت مظلة مؤسسة الحرس الثوري الإيراني (*Kagan&Stiansen,2015*).

من جهة أخرى، مارست مؤسسة الباسيج دوراً مماثلاً لممارسات الحرس الثوري الإيراني في شن الهجمات بالفضاء السيبراني على أهداف داخل الفضاء السيبراني الإيراني، وخارجه (رغم ادعائها بحصر جهود كوادرها في دائرة حماية الأهداف المدنية ومكاسب الثورة الإسلامية، داخل حدود إيران، من التهديدات والهجمات السيبرانية)، كما تحرص على توفير الموارد البشرية اللازمة لممارسة هجمات رفض الخدمة التي يروم الحرس الثوري ممارستها، والتي تتطلب مشاركة عدد كبير من المستخدمين في عمليات التعرض التي يتطلبها هذا النمط من الهجمات.

وتسخّر منظمة الباسيج بنيتها التحتية للمعلومات والاتصالات، والتي تمتد ضمن النسيج الشبكاتي لأكثر من ثلاثين محافظة إيرانية، لاستضافة مواقع ذات صبغة عسكرية، وترتبط بصورة غير معلنة بمؤسسة الحرس الثوري الإيراني، وتمارس دور القواعد السيبرانية لحرس الثوري، والعمود الفقاري لموارد جزء لا بأس به من قوة الردع السيبراني التي تدير دفتها من وراء الكواليس.

وفي خضم هذا النسيج المتشابك، والذي لا يكاد يفصح عن هوية الحضور السيبراني للعقد السيبرانية التي تلتحق بلبابه وأطرافه، تبرز على السطح شركة إيرانية، غير مشهورة، وتتمتع باستقلالية ظاهرية عن بقية الشركات التي تستضيف خدمة الإنترنيت في إيران، هي شركة *Ertebat Gostaran Bina* والتي كشفت التحريات عن دورها المشبوه في استضافة عنونة الإنترنيت لجميع المواقع التي ترتبط بصورة غير معلنة مع مؤسسة الحرس الثوري الإيراني، وتنفذ غاياته في الفضاء السيبراني الوطني والعولمي (*Kagan&Stiansen,2015*).

وقد ساهمت جامعة شريف للتقنية في دعم سعي النظام الإيراني للهيمنة على الفضاء السيبراني الإيراني من خلال إنتاج برمجيات ومعدات تقنية تساهم في مراقبة أنشطة المستخدمين الإيرانيين وتقطير مادة المحتوى السيبراني المطروح في فضاءات التواصل الاجتماعي[207]. كما أسهمت كوادرها المتخصصة في قطاع أمن المعلومات باستثمار البنية التحتية للمعلومات والاتصالات المتوفرة في مختبراتها لإطلاق حملة واسعة من التهديدات والهجمات السيبرانية على المعارضة الإيرانية في الداخل، وخصوم النظام في المنطقة، والولايات المتحدة، ودول أوربية. وقد أظهرت تحريات شبكة *Norse Intelligence Network* الاستخبارية أن التهديدات والهجمات السيبرانية التي تنطلق من هذه الجامعة العريقة لا تتخفى شأن ممارسات الفصائل السيبرانية للحرس الثوري الإيراني، وتنصبغ بعنونة الإنترنيت الخاصة بالفضاء السيبراني للجامعة، وتتوزع على أكثر من شبكة داخلية بالجامعة، الأمر الذي يؤكد حضور ممارسات فردية من أكثر من قسم من أقسامها أو مخابرها في ممارسة هذه الهجمات ضد الأهداف المنتخبة (*Kagan&Stiansen,2015*).

- **القسم الثالث:** هجمات تنشأ عن مضيفات خدمة، لم تتضح هوية الجهة التي تمتلكها وتدير نشاطها السيبراني، ولا تمتلك مواقع ويب، أو مضيفات خدمة البريد الإلكتروني، كما لا يمكن العثور على أسمائها،

[207] . أدرجت ثلاثة مخابر في جامعة شريف للتقنية على قوائم الحظر في الولايات المتحدة منذ عام 2012، بعدها أدرجت على قوائم الحظر لدول الاتحاد الأوربي في نهاية العام ذاته، وعادت كندا فأدرجتها ضمن قوائم الحظر بعد أن ثبت مساهمة هذه المخابر في دعم سعي الحكومة الإيرانية في مراقبة اتصالات المواطنين الإيرانيين، وإنتاج برمجيات مراقبة ذكية لتعزيز الحظر السيبراني بالبلاد (*Kagan&Stiansen,2015*).

وغيرها من التفاصيل التي يمكن أن تفصح عن هويتها، أو توفر بعض الدلائل عن طبيعة توطنها الجغرافي في فضاء الفيض السيبراني، وهوية الجهات التي تمتلكها أو تشرف على إدارة أنشطتها السيبرانية. ويمكن ربط هذه الموارد بالجهات المتحالفة مع النظام الإيراني، ووكلائها السيبرانيين الذين يمارسون نشاطاتهم في الجزء المظلم من فضاء الإنترنيت، داخل حدود إيران أو خارجها.

5. 3. أطوار السجال السيبراني ومجالاته في فضاء إيران السيبراني:

لم يتسن لإيران أن تلج فضاء المدافعة والنزاع السيبراني، دفعة واحدة، وإنما كان دخولها تدريجياً بفعل التغيرات التي نشبت في مراتب حضورها داخل حدود فضاء الفيض السيبراني المفتوح.

في البداية لم تتجاوز ممارسات المدافعة السيبرانية، داخل حدود الفضاء السيبراني الإيراني وخارجه، عن كونها ممارسات فردية حاول من خلالها المستخدمين إثبات قدراتهم على الولوج الى ساحة الحضور السيبراني للغير، فرداً كان أو مؤسسات، بقصد إثبات القدرة، أو إذكاء روح التحدي مع الغير، دون وجد تخطيط مسبق لإحداث ضرر أو تأثيرات تخريبية.

وقد مارس بعض المستخدمين لعبة المنازعة ونجحوا على صعيد اقتحام خصوصية بعض المواقع، أو إحداث خلل مؤقت فيها، واتسع نطاق المنازعة الفردية، قبل أن تنضج ممارساته، وتتحول شيئاً فشيئاً باتجاه تشكيل محيط المنازعة الذي بدأنا بتلمس مطالعه مع بدء انتشار الفايروسات الخبيثة، والبرمجيات الضارة في عموم الفضاء السيبراني العولمي، مع نضوج ممارسات القرصنة السيبرانية، وولادة جيل من الشيفرات الخبيثة التي نجح المستخدمون في طمرها بالمعمارية السيبرانية لإحداث تأثيرات ذات أثر ضار في مواقع الغير وتطبيقاتهم البرمجية.

ولا تكاد تختلف إيران في حضور فضاء المنازعة والمدافعة السيبراني في مجالها عن الإرهاصات التي بدأنا بتلمسها في عموم الفضاء العولمي، باستثناء البصمة الوطنية التي تشكّلت بفعل خطاطة النظام الإيراني تجاه حضور مواطنيها في هذا الف ضاء، والمحاولات المتكررة لسن نهج يتمتع بنكهة النظام الإيراني والأعراف التي يعدّها النظام مشروعة بحسب خطاطته القاهرة.

لقد أثمرت عمليات التنقيب التي مارسناها في الفضاء السيبراني الإيراني، وتحليل مادة وعناصر الحفريات السيبرانية التي حرصنا على مزاولتها، خلال مدة زمنية ليست بالقصيرة، داخل حدود هذا الفضاء الفريد عن العثور على ثلاث طبقات اتسمت كل منها بصبغة جعلتها تتميز عن أخواتها، نتيجة للظروف التي أفرزت تشكيل معالمها، وتحديد خصائصها الذاتية.

وقد حرصنا في عملية التقسيم على الحفاظ على خصوصية فضاء المنازعة والمدافعة الإيراني، مع تحديد العوامل التي أسهمت في نضوج الكثير من عناصره، ولعبت دوراً في تشكيل هويته المتميزة.

وقد لاحظنا أن الطور الأول للسجال السيبراني قد تشكّلت بداياته بعيد ولادة الثورة السيبرانية الخضراء عند التوطئة للانتخابات الرئاسية عام 2009، بينما انتهى حضوره مع بدء الهجمة الشرسة بواسطة الفايروس الخبيث *Stuxnet* الذي نجح ببلوغ أجهزة الطرد المركزي في مشروع نطنز النووي، بينما شهدنا ولادة الطور الثالث بعد نضج القدرات الهجومية في الفضاء السيبراني على استنسال أجيال جديدة من هذه البرمجيات الخبيثة، الأمر الذي أجبر إيران على

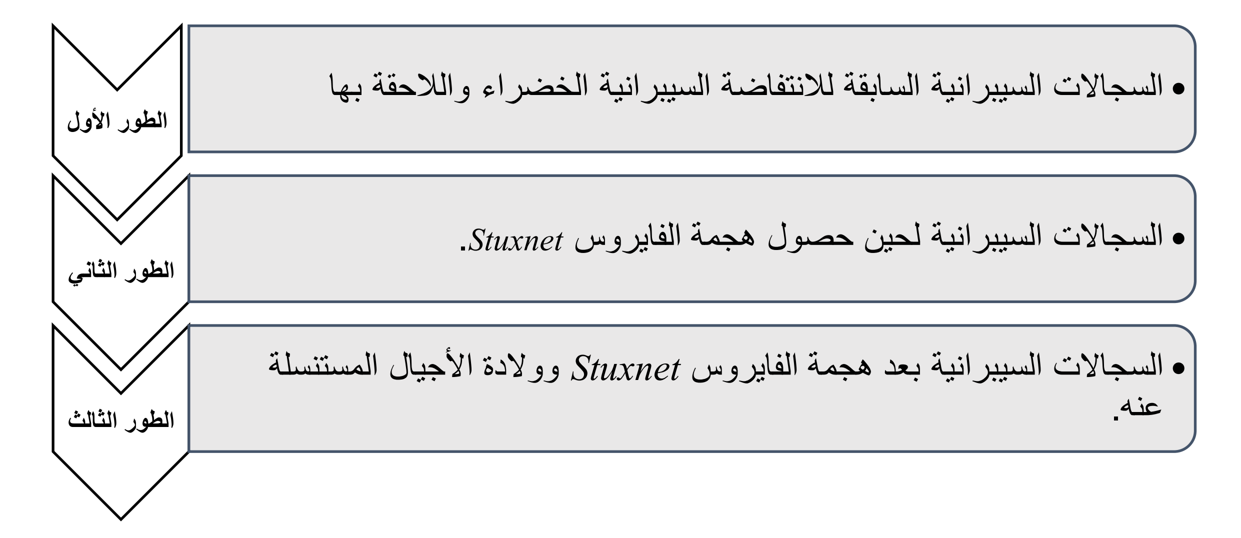
التوجه، بكل ما أوتيت من قوة لتشكيل مشهد الردع السيبراني الذي بدأ يتنامى الى الحد الذي نجح بتشكيل تهديد كبير على خصومها السيبرانيين، ثم لم يلبث أن يتطور بحيث أضحى يشكّل تهديداً على المستوى العولمي.

لقد عمدنا الى تقسيم هذه الأطوار الى ـ أنظر الشكل (6 - 1):

الطور الأول: السجالات السيبرانية السابقة للانتفاضة السيبرانية الخضراء واللاحقة بها.

الطور الثاني: السجالات السيبرانية لحين حصول هجمة الفايروس *Stuxnet*.

الطور الثالث: السجالات السيبرانية بعد ولادة الفايروس *Stuxnet* والأجيال المستنسلة عنه.



الشكل (6 -1) ـ الأطوار التي مرّت بها السجالات السيبرانية في فضاء الفيض السيبراني الإيراني.

ومن الملاحظ تقاصر البعد الزمني للقفز بين الطورين الأول والثاني، حيث استغرقت المدة الانتقالية بين الطور الأول والثاني عاماً واحداً فقط (العامين 2009 و2010)، وكذلك الحال بين الطورين الثاني والثالث لمدة سنتين، (الأعوام 2010 و2012)، بينما نتوقع أن يمر الطور الثالث بمراحل جديدة قد لا نفلح بتكهن نهاياتها مع التقدم المتسارع في تقنيات القرصنة السيبرانية وأدواتها، وعلى التوازي مع النزعة الإيرانية المحمومة لتطوير قدراتها على صعيد الدفاع والردع السيبراني.

وسنحاول أن نناقش في الفقرات القادمة تفاصيل عمليات السجال السيبراني، بمختلف أطوارها على صعيد المنازعة، والدفع والردع السيبراني لنوفر لقارئنا فرصة الاطلاع عن كثب على تطورها خلال أكثر من عقد من الزمن الذي احتشدت مدته بكم كبير من الأحداث المهمة والمتسارعة.

5 . 3 . 1 . السجالات السيبرانية السابقة للانتفاضة السيبرانية الخضراء واللاحقة بها:

بدأ النظام بممارسة أنشطة بدائية للسجال السيبراني في فضاء إيران السيبراني عندما باشر بتلمّس بدايات لتوجّه المعارضة الإيرانية نحو تسخير بعض ميزاته الفريدة في توطيد حضور خطابها في الفضاء المحلي، واستثمار هذه الميزات في تجاوز عقبات الرقابة والحظر، وممارسات الكبت التي زاولها النظام لتكميم أفواه المعارضة، وبلبلة خطابها، ومنعه من بلوغ طيف واسع من الجماهير الإيرانية.

وقد برر النظام ممارسات السجال السيبراني ـ الداخلي في إيران بقصد ضمان تماسك اللحمة الوطنية الإيرانية، والحفاظ على ثقافة الثورة الإيرانية بصبغتها الإسلامية المحافظة من الغزو الثقافي، وتهديدات الحروب اللينة التي باتت تمارسها دول الغرب لإحداث خلخلة في النسيج الاجتماعي الإيراني.

لم تتسم الهجمات التي مارستها فصائل النظام السيبرانية على المعارضة المحلية بالتعقيد، كما اقتصرت على توظيف تقنيات بدائية كانت كافية (خلال تلك الحقبة) على احتواء الحضور السيبراني للمعارضة وكف أنشطتها المختلفة. فشملت هذه الهجمات، هجمات رفض الخدمة لإغراق المواقع بسيل من النبضات السيبرانية وإيقافها عن العمل بصورة جزئية، أو مهاجمة تطبيقات منصات شبكات التواصل الاجتماعي، مثل: *Twitter&Facebook* لإيقافها، أو ممارسة عمليات الحظر السيبراني على التطبيقات ذاتها، أو إدراج رسائل تهديدية في مواقع المعارضة لترهيبهم ومنعهم من الاستمرار بممارسة الحضور المعارض (*Schwarz,2013*).

وفي الوقت ذاته، سعى النظام الى تسخير القدرات الكبيرة التي يتمتع بها قراصنة المعلومات الإيرانيين للمساهمة في السجال السيبراني المستعر مع المعارضة الإيرانية، فلم يخلو فضاء إيران السيبراني (منذ بداية الألفية الجديدة) من ممارسات القرصنة التي اتسمت بصبغة سياسية. ويلاحظ أن إدارات المواقع قد تلجأ الى الإفصاح عن أسباب هذه الهجمات وتلقي بالتهمة على الفئات المعارضة، من أحزاب أخرى، أو منافسين على ممارسة محددة تتعارض مع نهج جهات المعارضة، أو عند الترشح لمنصب سياسي مرموق في إيران. بينما تذهب جهات أخرى الى توجيه أصبع الاتهام الى مؤسسات حكومية محافظة، أو أخرى لها هيمنة داخل حدود المؤسسات الحكومية.

وتقاسمت كل من وزارة المخابرات الإيرانية (*MOI*) *Ministry of Intelligence* والحرس الثوري الإيراني مهمة السجال السيبراني مع المعارضة الإيرانية في داخل البلاد، وذلك عن طريق المراقبة المستمرة لخطاب التواصل الذي يسافر عبر قنوات الرسائل القصيرة في الهواتف المحمولة، والتنصت على المكالمات الهاتف، أو استخدام أدوات وبرمجيات التلصص الإلكتروني على جميع قنوات التواصل السيبراني بين المواطنين الإيرانيين الذين تحوم حولهم الشبهات لتوفير أدلة كافية للقبض عليهم وتطبيق قوانين الجرائم السيبرانية ـ الصارمة بحقهم (*FWC,2015*).

وتلجأ هذه الجهات، في أحيان أخرى، الى توظيف مصائد إلكترونية للمعارضة الإيرانية عن طريق بث منشورات، أو تغريدات، أو صور، أو صناعة حسابات وهمية بأسماء قادة المعارضة وناشطيها المشهورين، بقصد استدراج البعض والإيقاع بهم. ويضاف الى كل ذلك وجود تطبيقات المراقبة والحظر الذكي الذي يمارس عملية الحظر والكف السيبراني على مادة المحتوى السيبراني الذي يعارض خطاب النظام الإيراني ليزيح هذه الخطابات من فضاء التواصل الإيراني ويحول دون انتشاره أو تداوله بصورة واسعة بين المستخدمين الإيرانيين.

وقد التحقت الميليشيات السيبرانية للباسيج[208]، وشرطة فضاء إيران السيبراني، بجحافل الفصائل التي نهضت للمشاركة بالسجال السيبراني الداخلي ضد المعارضة الإيرانية التي أفلحت في 2009 في ترسيخ بصمة حضورها السيبراني ـ المعارض.

208 . ذكر علي فاضلي، المدير التنفيذي لمؤسسة الباسيج، أن قراصنة المعلومات الذين يعملون بمعية مؤسسته قد قاموا بسلسلة هجمات على مواقع ويب يستخدمها أعداء إيران لشن حرب ناعمة ضد الثورة الإسلامية في إيران، ولضمان حماية أمن معلومات الفضاء السيبراني بالبلاد من حملات التشويه. وأكد أن مؤسسة الباسيج تعمل جاهدة ومن خلال الدعم الذي تقدمه الى قسم تقنية المعلومات والاتصالات الملحق بها لمواجهة التهديدات السيبرانية المتزايدة التي تستهدف إيران في أكثر من مجال من مجالات حروب المعلومات، وأنه لولا هذه الجهود الحثيثة فإن إيران لن تكون قادرة على درء التهديدات المتلاحقة على بنيتها التحتية وأمنها السيبراني الوطني. وقد شدد على الدور المهم الذي يمارسه الجيش السيبراني الذي يعمل مع

كما أن مجاميع قراصنة المعلومات التي توالي النظام قد أعلنت التحاقها بهذه المجاميع، بعد أن صرّح بيروز كماليان في شهر أيار عام 2013 أن مجموعة *Ashiyane* (التي تعد المجموعة الأكثر تطوراً على صعيد القرصنة السيبرانية في إيران) باتت ملتزمة بحماية إيران من القرصنة السيبرانية والهجمات المتكررة على المواقع الحكومية، ودرء الأكاذيب التي تمارسها القوة الناعمة لتضليل الرأي العام، وتشويه صورة الثورة الإسلامية داخل البلاد وخارجها (*HP,2014*).

كان الفضاء السيبراني الإيراني، في بداياته، مفتوحاً أمام نشاط قراصنة المعلومات، الأمر الذي شجع من يتقنون صنعة القرصنة السيبرانية، والمبتدئين، على ممارسة أنشطة بدائية لاختراق مواقع وحسابات لمستخدمين إيرانيين، وآخرين خارج حدود الفضاء المحلي، ليثبتوا لأقرانهم قدراتهم على صعيد القرصنة[209]، أو يعبروا عن نزعتهم الوطنية، أو يفصحون عن ولائهم لخطاطة الثورة الإسلامية في إيران[210].

بدأت مجموعة قراصنة المعلومات نشاطاتها منذ عام 2002 بعد أن أرسى بيروز كماليان، رئيس المجموعة، أهدافاً محددة للمجموعة تضمنت تحسين الحصانة الأمنية لمواقع الويب في الفضاء السيبراني الإيراني. بيد أن عمل والده في مؤسسات إيرانية مهمة قد صبغ توجهاته نحو إعلان ولائه لخطاطة النظام الإيراني، والتوجه تدريجياً نحو توجيه مسارات مجموعته نحو حماية مكتسبات النظام، ودرء المخاطر التي تحيق بحضوره وبكياناته السيبرانية التي تستوطن الفضاء السيبراني.

وعثرنا في حفريات الحضور السيبراني لهذه المجموعة على بصمات متعددة لسلسلة من الهجمات، خلال عام 2005، التي استهدفت مواقع ويب تعود للإدارة الأمريكية بقصد التعبير عن رفض التهم التي وجهتها الإدارة الأمريكية لوجود بصمات مشاركة للنظام الإيراني في هجمات 11 من سبتمبر، ثم توسيع رقعة الهجمات لتنال بضعة مواقع تعود الى وكالة الفضاء الأمريكية *NASA* (*Kagan&Stiansen,2015*).

واستمرت هذه المجموعة بتسخير طاقات ومهارات قراصنتها لخدمة النظام وحمايته من التهديدات الداخلية، والخارجية، على حد سواء. ولقد لعب كماليان دوراً مهماً أثناء الاضطرابات التي رافقت الحملة الانتخابية عام 2009 بعد أن وفر سجلاً ثميناً من البيانات الشخصية لأفراد المعارضة الإيرانية الذين استخدموا منصات التواصل الاجتماعي لنشر تغريداتهم، ومنشوراتهم للمّ صفوفهم وتأجيج اعتراضاتهم ضد اختراقات السلطة وممارساتها القمعية، مما دعم الحرس الثوري الإيراني وبقية المؤسسات الأمنية الحكومية في إلقاء القبض عليهم خلال مدة زمنية قصيرة (*Kagan&Stiansen,2015*).

كذلك وجهت أصابع الاتهام الى مجاميع قراصنة المعلومات الموالية للنظام الإيراني في شن سلسلة هجمات معلوماتية على أهداف منتخبة في الفضاء السيبراني الصهيوني شملت: سوق تل أبيب للأوراق المالية، وخطوط العال الجوية، ومواقع ويب تعود الى بنك إسرائيل الدولي، ومصرفي *Massad & Otzar Hahayal*.

مؤسسة الباسيج، والذي يتألف من مجموعة من أساتذة الجامعة، والطلبة المتميزين بالمؤسسة الجامعية والحوزات العلمية، ممن نذروا قدراتهم وخبراتهم السيبرانية لدرء الأخطار المحدقة بإيران من أعدائها (*MAI,2011*).

[209] . قامت مجموعة قراصنة الإمبراطور *Emperor Team* بقرصنة مجموعة من مواقع الويب والنطاقات الثانوية لمواقع شهيرة مثل *MSN, Yahoo and Back-box* خلال الأعوام 2002-2004 بقصد نيل الشهرة وتسليط الأضواء على مجموعتهم في مجتمع قراصنة المعلومات العولمي (*IICT,2013*).

[210] . نلاحظ الكثير من الهجمات السيبرانية التي تمارس فيها عمليات ملاحقة أصحاب وإدارات المواقع المخالفة للشريعة الإسلامية، أو المناهضة لثقافة الثورة الإسلامية التي يتبناها النظام الإيراني، ويسارع الى قرصنة مواقعهم على الويب، مع ممارسة عملية حظر المحتوى المطروح فيها[210](*IHRO,2014*).

ولاحظنا وجود علاقة مباشرة بين تزايد الهجمات على المواقع الصهيونية، على التوازي، مع شن الكيان الصهيوني لهجمات عسكرية ضد الفلسطينيين المقيمين في قطاع غزة المحتل[211]. حيث بلغ عدد الحواسب التي مارست هجمات رفض الخدمة (في شهر يناير عام 2009) حوالي خمسة ملايين حاسب، تعود الى قراصنة معلومات منتمين الى حركة حماس، وحزب الله اللبناني، وآخرين من إيران. وقد تطورت هذه الهجمات فناهزت أكثر من 900,000 هجمة معلوماتية توزعت في الفضاء السيبراني الإسرائيلي عندما تأجج الصراع في قطاع غزة عام 2014 (*Edge Wave,2015*).

ويحفل ملف السجال السيبراني المحلي بكثير من الأحداث التي تصف بقية محاور النزاع السيبراني وتوجهاته خلال عقد من الزمان. فأثناء اندلاع الاحتجاجات المصاحبة للحركة الخضراء المناهضة لنظام الرئيس الإيراني السابق محمود أحمدي نجاد، عام 2010، قامت المعارضة الإيرانية بتوظيف خدمة تحديث صفحة الخدمة *Page Refreshing Service* لممارسة هجمات رفض الخدمة على موقع الرئيس المذكور من داخل إيران باستخدام برمجيات مجانية متوفرة على شبكة الإنترنيت، وفي الوقت ذاته مارست المعارضة المقيمة من خارج إيران هجمات رفض الخدمة عبر بوابات تطبيقات شبكات التواصل الاجتماعي، الأمر الذي أجبر النظام الإيراني على حظر هذه المواقع لتقليل التأثيرات المصاحبة لهذه الهجمات على مواقعه المختلفة[212] (*Zuckerman,et., al.,2010*).

وفي شهر فبراير من عام 2013 قامت مجموعة الجهاد الافتراضية ـ المستقلة *Virtual Anonymous Jihad* باجتياح وإيقاف موقعين يرتبطان بصورة مباشرة مع الرئيس الإيراني السابق والمعارض للنظام الإيراني (المقيم في فرنسا) أبو الحسن بن صدر (*Enghelabe-eslami.com& Banisadr.org*). وعاودت المجموعة باكتساح موقع لقناة تلفزيونية *Irtv.com* بالولايات المتحدة، تعود للمعارضة الإيرانية خلال شهر أيار من العام ذاته، ثم باشرت هجمات متعددة في شهر يونيو، وقبيل بدء الانتخابات الرئاسية بإيران، انقضّت فيها على مواقع (*Digraban.com,Khodnevis.org&Ostanban.com*) والتي استضيفت خارج حدود إيران، وتعود الى شخصيات تعارض النظام الإيراني، وأوقفتها عن العمل، مع إيداع رسالة تحذيرية تنبّه المعارضين الى عدم قدرتهم على الإفلات من قبضة حزب الله الإيراني حيثما حلوا وارتحلوا (*Mansharof,2013*).

وقامت مجموعتان من قراصنة المعلومات الإيرانيين هما *Cadelle and Chafer* (خلال عام 2014) بالتجسس على مجموعة من المواطنين الإيرانيين، ومؤسسات تعود الى قطاعي الطيران والاتصالات في دول الشرق الأوسط باستخدام تقنية *Backdoor* (*Symantec,2015*) كذلك، أجهز القراصنة على موقع اتحاد الطلبة الإصلاحيين في جامعة أمير أكبر للتقنية، وموقع المسار الأخضر *Rah-e Sabz* الذي يدعم النهج الإصلاحي للمعارض مير حسين موسوي (*Zimmt,2010*).

أما أثناء حملة الانتخابات الرئاسية لعام 2013 فقد شن جيش فضاء إيران السيبراني بضعة عشر هجمة على مواقع المعارضة الإيرانية التي تعمل في فضاء إيران السيبراني، مثل: موقع صوت الأهواز، وموقع أهواز الحرة، وموقع المعارضة

[211] . نجح قراصنة مجموعة *Ashiyane* بشن سلسلة هجمات شرسة على مواقع ويب إسرائيلية خلال العقود الماضية، شملت: موقع الموساد، وموقع وزير الدفاع الإسرائيلي السابق أيهود باراك (*Hemmat&Ellett,2011*).

[212] . أدعت مجموعة الإمبراطور قيامها باختراق اثنين من مرشحي الحملة الانتخابية الرئاسية لعام 2005 أثناء عمليات الاقتراع لصالح مرشح آخر (*IICT,2013*).

الانفصالية بالأهواز، ومدونة الصحفي الإيراني آراش سيكارجي، وموقع إيران العولمي، ومواقع أخرى تدار بواسطة المعارضة داخل إيران أو خارجها .(*Mansharof,2013*).

ولم تخل ممارسات القرصنة في إيران من ممارسات جرمية سعى أصحابها الى ابتزاز مستخدمين، أو شركات ومؤسسات مالية، أو توفير خدمات لشركات متنافسة للتأثير على منافسيهم في السوق والأنشطة المالية. وتفصح الوثائق عن كثير من هذه الممارسات منها قيام مجموعة قراصنة الإمبراطور أنها قد تلقت عرضاً من إحدى الشركات الإيرانية فبدأت باختراق قاعدة بيانات لدى إحدى المؤسسات الحكومية، والتي توفرت في مضيف رقمي يقيم في مقر تلك المؤسسة، ضمن عملية أمنية استغرقت شهراً كاملاً(*IICT,2013*).

5 . 3 . 2 . السجالات السيبرانية لحين حصول هجمة الفايروس *Stuxnet*:

تطورت أنماط السجال السيبراني في هذه المرحلة عما كانت عليه في الطور الأول، وهرع قراصنة المعلومات الذين يعملون بصورة مستقلة عن خطاطة النظام الإيراني، والملتحقين بها، والمليشيات السيبرانية المنتسبة الى مؤسسة الحرس الثوري الإيراني، ومنظمة الباسيج، وفصائل جيش إيران السيبراني الى تطوير مهاراتهم وتوظيف تقنيات متقدمة في ممارسة التهديدات والهجمات، وانتخاب أهداف مهمة، مع تطوير عناصر سيناريو ممارسة الهجمات، وتعميق التحالفات فيما بينهم لضمان عمق تأثيرها على خصومهم داخل إيران وخارجها.

واستمر السجال السيبراني في بدايات هذا التطور على نفس المنوال بين عمليات كرّ وفرّ مارستها الفصائل السيبرانية الملتحقة بكلا المعسكرين المتخاصمين، ولم تؤشر في وقائع هذا السجال غلبة لفريق على آخر، ولم تكن آثار هذه الهجمات جسيمة، بل كانت ذات تأثير سطحي، ومؤقت، بحيث لم تورث صنّاع القرار لدى الجهات المتصارعة قلقاً كبيراً، ولم تتطلب إحداث تغييرات كبيرة في السياسات التي تنتهجها في إدارة ملفها الأمني بالفضاء السيبراني.

وقد أفاق العالم أجمع، بنفس توقيت الصحوة الإيرانية، على التسريبات التي تناقلتها وسائل الإعلام حول الهجمة الشرسة التي مورست ضد منشآت تخصيب اليورانيوم ـ الإيرانية بواسطة الفايروس الخبيث *Stuxnet* والتي كان لها دور كبير في إحداث تغييرات جوهرية وحاسمة في سياسة واستراتيجية أمن المعلومات لدى النظام الإيراني، كما ألقت بالوقت ذاته بآثار كبيرة على المشهد العولمي لممارسات التهديدات السيبرانية في عموم الرقعة الجغرافية التي يمتد عليها الفضاء السيبراني العولمي.

وقد انتشلت هذه الصفعة السيبرانية المدوّية النظام الإيراني من آفة الغرور التي لازمت خطابات الكثير من قياداته العسكرية والأمنية، والتقنية، بالإضافة الى الخطاب المتعالي الذي صدعت به قيادات من الحوزة العلمية حول حصانة الفضاء الإيراني ضد هجمات الخصوم، ووعورة مسالكه تجاه محاولات أعداء إيران عند محاولة التغلغل فيه[213]. وأسهمت هذه الهجمة، بالوقت ذاته، في إحداث صحوة، وطفرة غير مسبوقة، لدى الإدارة الحكومية الإيرانية بالتوجه نحو تعزيز قدراتها الدفاعية السيبرانية، والسعي الحثيث نحو تطوير قدراتها الهجومية بحيث يمكننا القول إن مقدار

[213] . أدّعت مؤسسة الحرس الثوري الإيراني، منذ بضع سنين، على لسان أكثر من قيادي من قيادييها المرموقين، أن طهران قد نجحت في تطوير سلطانها السيبراني الى مستوى سيجعلها قادرة على اختراق البنى التحتية الأساسية التي تعود الى المؤسسات العسكرية للدول التي تناصبها العداء معلنة البدء بتشكيل قوة رقمية ضاربة، تدعم القوة الدفاعية التي تسهر على حماية كيانات إيران السيبرانية من الهجمات التي تحاول النيل منها في الفضاء المتخيّل(*Mansharof,2013*).

الأضرار المترتبة عن تغلغل هذا الفايروس في البنى التحتية للمعلومات والاتصالات الإيرانية لم تعد تصلح للمقارنة مع مقدار ما جنته وما يمكن لها أن تجنيه من تنامي في قدراتها السيبرانية وسلطانها السيبراني.

كانت هجمة هذا الفايروس الفريد صفعة مدوية ودرساً بليغاً، للنظام الإيراني، وبجميع مفاصله، أيقظت في كيانه مارداً رقمياً سيبقى مصدراً يقضّ مضاجع الدول المناهضة، ويغيّب الفرحة عما تحقق من هذه الهجمات نتيجة لحجم المخاطر التي ستنشب عن هذه الصحوة غير المتوقعة.

لم تحصل ولادة هذا الفايروس الخبيث، وانطلاقة هجمته الشرسة، دفعة واحدة، ولكنها مرّت بسلسلة من التطورات لحين استكمال سيناريو الهجمة، وتغلغل الفايروس *Stuxnet* الى عمق وحدات التحكم بتشغيل أجهزة الطرد المركزي لمشروع نطنز النووي ـ الإيراني[214].

وتشير التقارير المتوفرة بين أيدينا الى أن المعمارية البرمجية للفايروس *Stuxnet* قد بوشر بإنشائها وتطوير خوارزمياتها منذ عام 2005 وبواسطة فريق مشترك من وكالة المخابرات المركزية بالولايات المتحدة والوحدة الخاصة 8200 في إسرائيل. وقد أنشئت وحدة ريادية *Pilot Plant* مشابهة لمنظومة أجهزة الطرد المركزي الإيرانية من على أجهزة طرد مركزية صنعت في باكستان واستخدمت في إحدى الوحدات النووية بليبيا، لاختبار مستوى نجاعة السلوك الخبيث للفايروس، وإجراء سلسلة من التعديلات البرمجية لبلوغ مستوى رصين من الأداء وتنفيذ المهام التي أنيطت بمعماريته ومنطقه البرمجي (*Salvin&Healy,2014*).

ورغم أن الجهة التي صنعت الآفة، أرادت لها ألا تصيب إلا أجهزة الطرد المركزي الإيرانية، وأجهزة التحكم التي صنّعت في شركة *Siemens* الألمانية، دون غيرها، إلا أن هفوة ارتكبها أحد العلماء الإيرانيين (بربط حاسوبه المصاب بصورة مباشرة مع شبكة الإنترنيت) قد تسببت بسفر الآفة وتسللها خلسة عبر شبكة الإنترنيت وانتقالها الى مشاريع أخرى في إيران، قبل أن تهاجر الى بلدان أخرى، منها ألمانيا، وإندونيسيا، والهند، وباكستان، واستمرت في رحلتها حتى بلغت البلد الأم الذي ولدت فيه، الولايات المتحدة (*Salvin&Healy,2014*).

---

[214] . استطاع أحد المتخصصين في تحليل معمارية البرمجيات الخبيثة (والذي أمضى أكثر من عامين في عملية التحليل والمراجعة) العثور على شيفرة برمجية في فايروس *Stuxnet* الذي هاجم المنشآت النووية الإيرانية تعود بصمتها الى عام 2006. وقد أعدّ جدولة زمنية لعملية مهاجمة أجهزة الطرد المركزي في مشروع نطنز النووي، وكما يأتي (*Finkle,2011*):

- أكمل المهندسون في أيار 2006 تشكيل هيكلة الشيفرة البرمجية للفايروس *Stuxnet* الذي خطط له إنجاز الهجمات ضد متحكمات أجهزة الطرد المركزي لشركة *Siemens*.
- أقحم البرنامج الخبيث *Duqu* عام 2007 لمهاجمة أهداف منتخبة في إيران، لسرقة بيانات حيوية.
- في نهاية عام 2007 أكمل المهندسون العمل على إعداد شيفرة لقنبلة رقمية أودعت في فايروس *Stuxnet* للعبث ببرنامج تشغيل أجهزة الطرد المركزي والتحكم بسرعها.
- في ديسمبر 2008 قام العاملون على الفايروس الخبيث بتشغيل موقع الويب الذي سيمارس دور الوسيط بين أجهزة التحكم والأجهزة التي طالتها آفة الفايروس.
- استمر العمل في شهر يناير من عام 2009 على مراجعة تشغيل الموقع الجديد، واستكمال كتابة مجموعة من الإيعازات المهمة للفايروس الخبيث.
- في مارس 2009 استكمل العمل على الأداة التي ستنقل الفايروس الى المنشآت المستهدفة في إيران، حيث مارس الفايروس نشاطه على التوازي مع مناسبة مرور ثلثين عاماً على ولادة الثورة الإسلامية.
- في يناير 2010 قام المشغلون بتسريع نشاط الفايروس عن طريق إضافة برنامج خبيث جديد ساعد على نشر الآفة بسرعة أكبر، وزيادة حجم المخاطر المترتبة عن الإصابة به.
- في مارس من العام ذاته استحدثت تطويرات جديدة في المعمارية البرمجية للفايروس مع تعميق قدراته التأثيرية.
- في يونيو 2010 عثر على بصمة الفايروس بعد تحليل حضورها في إيران.

في سبتمبر 2010 أفصح رئيس جمهورية إيران السابق، محمود أحمدي نجاد عن توظيف سلاح رقمي لإحداث عملية تخريب في أجهزة الطرد المركزي في المشروع النووي الإيراني، وأن أجهزة المعلومات الإيرانية قد نجحت في الكشف عن هذه الهجمة.

ولم تتوقف التهديدات عند حدود هذه الهجمة التي أصابت أكثر من 100 ألف نظام محوسب ضمن حدود إيران (*Mele,2013*)، بل توسعت باتجاه توليد المزيد من الأنسال التي حاكى المبرمجون فيها معمارية فايروس *Stuxnet* مع إضافة المزيد من التأثيرات الأكثر ضرراً، مع توسيع دائرة التأثير على حقول قطاعات متعددة.

فشهدنا مولد البرنامج الخبيث *COMODO* في عام 2011، ثم تلاه ولادة الفايروس الخبيث *DUQU* في السنة ذاتها، ثم جاءت ولادة كل من البرنامجين الخبيثين *FLAME* و*GAUSS* في عام 2013 والتي حرثت البنية التحتية للمعلومات والاتصالات، والكثير من الكيانات السيبرانية المهمة في إيران طولاً وعرضاً[215].

كانت ولادة الفايروس *Stuxnet* (والنجاح الكبير الذي حققه على صعيد التأثير على برنامج إيران النووي) وبعد قيام الشركات المتخصصة بمكافحة آثار الفايروسات بنشر تفاصيل معماريته البرمجية، والشيفرات المودعة فيه، ايذاناً بولادة مرحلة جديدة، بدأنا نشهد فيها ولادات جديدة لفايروسات استنسلت معماريتها من المنطق الفريد الذي ساد معماريته البرمجية.

وأعلن مخبر التشفير وأمن نظم المعلومات *CrySyS* في جامعة بودابست للتقنية والاقتصاد، في شهر سبتمبر من عام 2011 العثور على برنامج خبيث من فئة حصان طروادة *Trojan Horse* أعدت خوارزمياته البرمجية للتجسس على منظومات التحكم في المنشآت الصناعية بمنطقة الشرق الأوسط، والذي أطلق عليه اسم *DUQU*. ولم تمر سوى مدة يسيرة حتى أعلنت السلطات الإيرانية عن العثور على هذا البرنامج الخبيث بعد أن أحكم إصابته على مجموعة من نظم الإدارة الصناعية ببعض منشآتها (*Knopová&Knopová,2014*).

وفي شهر أغسطس من عام 2012 عثرت مختبرات شركة *Kaspersky* الروسية، والمتخصصة بالكشف عن البرمجيات الخبيثة ومحاربتها على برنامج خبيث ينتمي الى أسرة *Stuxnet* يمارس مهمة التلصص على عمليات تحويل الأموال في مصارف محددة، أطلق عليه اسم *Gauss Trojan*.

وشأن الأب الروحي لهذه البرمجيات الخبيثة *Stuxnet* لم تمارس البرمجيات الخبيثة الجديدة التي استنسلت من معماريته البرمجية، مثل *Flame*، *DUQU*، *Gauss* أي نشاط أو ممارسة خرجت عن نطاق سلوك محدد، باتجاه منظومات معينة، ولممارسة تأثيرات ذات طابع استراتيجي لا تقوم به إلا مؤسسات حكومية تروم إحداث تأثيرات تفصح عن نهجها ضد خصومها وبرامجهم التي قد تتعارض مع خطاطتها الاستراتيجية أو الأمنية، أو السياسية (*Knopová&Knopová,2014*).

وعدّ البرنامج الخبيث *Flame* من أخطر ذراري الفايروس *Stuxnet* بعد أن أثبتت عملية تحليل معماريته البرمجية عن تطور المنطق الذي استخدم في صياغة خوارزمياته بحيث أطلقت عليه الكوادر العاملة في مختبرات شركة

[215] . شملت قائمة السلالة التي انبثقت عن المعمارية البرمجية لفايروس *Stuxnet* كل من فايروس: *Flame*، *DuQu*، *Mahdi*، *Gauss*، *Rocra*، *FinFisher* والتي تمثل الجيل التالي "*Heirs/ Children*" من البرمجيات الخبيثة (*Mele,2013*).

Kaspersky الفايروس الذي يستبطن في بنيته البرمجية جميع أنماط السلوك التي تمارسها البرمجيات الخبيثة عبر تاريخها الطويل[216] (*Kaspersky,2016*).

ولم تقف الإدارة الحكومية الإيرانية، وفصائلها السيبرانية المتكاثرة، مكتوفة الأيدي، قبالة هذا التصعيد غير المسبوق على حزمة متنوعة من الكيانات السيبرانية التي استوطنت في رقع جيوسياسية وتقنية متعددة بعموم مساحة الفضاء السيبراني الإيراني.

وقد تعاملت الإدارة الحكومية للرئيس حسن روحاني بجدية مع آثار الهجمات السيبرانية الشرسة التي كانت بدايتها مع الفايروس الخبيث *Stuxnet* في عام 2010، وما جاء من بعده من سلالات استهدفت أهدافاً حيوية واستراتيجية في إيران، ثم ولادة التهديد الذي صاحب البرنامج الخبيث *WIPER* والذي اجتاح نظم معلومات وزارة النفط الإيرانية وشركاتها ومنصات تصدير النفط، في عام 2012، الأمر الذي أجبر حكومة حسن روحاني نحو التوجه الى زيادة حجم التخصيصات الاستثمارية لتطوير أمن فضاء الفيض السيبراني بما يتناسب مع ازدياد حجم التهديدات، فازدادت نسبة التخصيصات بنسبة 1200% خلال السنوات المالية الثلاث 2014-2015- 2016 (*Lasiello,2015*).

وبعد مرور خمسة أشهر على الهجمة الشرسة لفايروس *Stuxnet* على المنشآت النووية الإيرانية، قامت مؤسسة الحرس الثوري الإيراني وبالتنسيق مع منظمة الباسيج بتدريب 1,500 مقاتل رقمي *Cyber Warrior* وبدأ الطلب على قراصنة المعلومات والمتخصصين بممارسة حرفة اختراق المواقع، مع تشجيع الشباب على التوجه الى الالتحاق بنوادي القرصنة السيبرانية[217]، الأمر الذي دفع الكثير من الشباب الإيرانيين الى التوجه نحو الكليات والمعاهد المتخصصة في اختصاص أمن شبكات الحواسب، وتنمية القدرات على اختراقها، واكتشاف الثغرات الأمنية المقيمة في نسيجها الشبكاتي، وذلك لتوفر دعم حكومي للمتفوقين، مع إمكانية نيل فرصة عمل أكيدة لدى اكثر من مؤسسة حكومية (*INSS,2015*).

وقد بدت بالأفق نتائج التوجهات السريعة والمحمومة للنظام الإيراني، والفصائل السيبرانية الملتحقة بمؤسساته والموالية له، ونضجت ثمارها بحيث بدأنا نلاحظ بزوغ الكثير من الهجمات السيبرانية، ونجاح الفصائل وقراصنة المعلومات الإيرانيين باجتياح كم كبير من مواقع الجهات التي أسهمت في صناعة البرمجيات الخبيثة التي اجتاحت حواسب المشروع النووي الإيراني، ومواقع الدول المناوئة للنظام في المعسكر الغربي ومنطقة الشرق الأوسط.

كان لجيش فضاء إيران السيبراني، والفصائل التي عملت بمعيته، قصب السبق على صعيد تصعيد الهجمات السيبرانية، بعد أن نجح فايروس *Stuxnet* بتحقيق خلل تقني في أجهزة الطرد المركزي بالمشروع النووي الإيراني، بالإضافة الى التهديدات التي نشبت عن ذراريه وأنساله المتلاحقة.

---

[216] . أثبتت التحريات أن هذا البرنامج الخبيث قادر على ممارسة دور كل من: حصان طروادة، ودودة خبيثة، ومهمة التلصص السيبراني، مع إمكانية انتقاله عبر مجموعة متنوعة من الوسائط، وممارسة مهام متعددة بحسب رغبة الجهة التي قامت بابتكاره. فيقوم بجمع البيانات، والتقاط صور حية لشاشات التحكم، والهيمنة على منطق تشغيل المعدات الصناعية، وتسجيل المحادثات الصوتية، أو تحقيق الارتباط بواسطة معدات *Bluetooth* لنقل البيانات الى مستودعات آمنة.

[217] . أعلنت المنظمة الإيرانية للدفاع السلبي *Iran's Passive Civil Defense Organization*، وفي منتصف شهر يونيو 2010، أن لديها خطة متماسكة لتجنيد قراصنة المعلومات الإيرانيين وتهيئتهم للبدء بممارسة أنشطة الحرب اللينة *Soft War* (*HP,2014,a*).

بدأ الحرس الثوري الإيراني بتطوير قدراته السيبرانية في محوري الدفاع وممارسة التهديدات والهجمات السيبرانية منذ عام 2005، غير أن أوان نضجها لم يحن إلا بعد الصحوة التي فرضت عنوة على إيران بعد الهجمة التي اجتاحت منظومات التحكم في مشروع نطنز النووي، وتكاثر سلالات الفايروسات الخبيثة التي باتت تهدد الأمن القومي الإيراني(*Connell,2014*).

أسهمت القدرات التقنية المتقدمة التي يمتلكها أفراد جيش فضاء إيران السيبراني في ممارسة سلسلة هجمات معلوماتية طالت كيانات معلوماتية، كانت بمنأى عن التهديدات والهجمات التقليدية التي تمارسها مجاميع قراصنة المعلومات التي تعمل بصورة منفردة. فقد نجحت فصائله في اقتحام مواقع حكومية حصينة لأكثر من دولة عظمى، وعلى رأسها الولايات المتحدة الأمريكية[218]، واكتسحت العديد من مواقع الإعلام والصحافة الغربية، كما ولم تسلم من هجماتها منصات شبكات التواصل الاجتماعي العملاقة بعد أن حققت اختراقاً نوعياً لمنصة التغريد السيبراني *Twitter* (*BBC,2013*).

في البداية، لم تكن فصائل جيش فضاء إيران السيبراني قادرة على اختراق مضيفات خدمة مواقع الويب، وتركزت هجماتها على توظيف تقنية قرصنة بدائية، استهدفت سرقة أسماء نطاقاتها واستخدام أسماء نطاقات مزيفة لتغيير مسارات المرور السيبراني لمدة زمنية قصيرة، الأمر الذي قلل من التأثير المصاحب لهذه الهجمات وتأثيراتها المؤقتة. بيد أن وقائع القرصنة التي بوشرت على موقع التغريد السيبراني *Twitter* في النصف الثاني من عام 2010 أكدت حصول طفرة في تقنيات القرصنة التي وظفت في الهجمات الجديدة، بحيث نجح قراصنة المجموعة في إحداث تأثيرات أكثر ضرراً. وقد أشار أحد الباحثين الى أن هذه الطريقة تشابه الى حد كبير النهج الذي استعمله أحد قراصنة المعلومات الإيرانيين عند محاولته مواقع ويب وكالة الفضاء الأمريكية *NASA* الأمر الذي يؤكد التنسيق المستمر بين قراصنة المعلومات وجيش فضاء إيران السيبراني، أو ممارسة الهجمة من قبل القراصنة تحت مظلة جيش إيران السيبراني (*Rezvaniyeh,2010*).

لقد تطورت تقنية القرصنة السيبرانية لدى فصائل جيش فضاء إيران السيبراني، حيث لم تعد تقتصر هجماته مقتصره على استخدام تقنية رفض الخدمة *DDoS* والتي ينشب عنها إيقاف الموقع المستهدف لبضعة ساعات)كما حصل مع موقع التغريد *Twitter* وموقع محرك البحث الصيني (*Baidu*، فقد أثبتت الدراسات التي قامت بها بعض مراكز البحوث الأمريكية أن الهجمة التي استهدفت موقع محطة إذاعة صوت أمريكا *VOA* خلال عام 2011 وموقع *Tec.Crunch* أن سيناريو الهجمة لم يقتصر على إحداث التوقف المؤقت بالموقع، وإنما استمرت الهجمة بقيام مضيف الجيش السيبراني بزج برنامج خبيث *Botnet* في الموقع المستهدف بلغت تأثيراته الى حواسب المستخدمين عن طريق زرع ثغرة أمنية تتيح للفصائل المهاجمة فرصة التحكم بنظام التشغيل، ولوحة تحكم مستخدم أكثر من 400 ألف حاسب أصيب بآثار هذه الهجمة الخبيثة (*Shakarian,et.,al.,2013*).

[218]. في شهر ديسمبر من عام 2011 أعرب المدير التنفيذي لشركة *Google* العملاقة عن انبهاره بالقدرات السيبرانية التي يمتلكها أفراد جيش إيران السيبراني، عندما أعلن في مقابلة متلفزة في قناة *CNN* عن قيامهم بقرصنة الفيض السيبراني المسافر نحو الدانمرك وتغيير مساره باتجاه فضاء إيران السيبراني، ومن ثم إعادته الى الدانمرك ثانية، ودوون علم الأخيرة بهذه العملية (*BBC,2013*).

لقد استثمر هذا النهج من القرصنة في الهجمات التي شنت على مواقع الحركة الخضراء، فوفر لأفراد الجيش السيبراني فرصة إضافية في التوغل بحواسب المعارضة والكشف عن هوياتهم، وجمع الكثير من المعلومات التي دعمت الشرطة السيبرانية في إلقاء القبض عليهم.

كذلك يلاحظ كثرة استخدام هذا النمط من الهجمات على مجموعة من المصارف الأمريكية خلال الربع الأخير من عام 2012، منها: مؤسسة مصرف أميركا، ومصرف *JP Morgan Chase*، ومصرف *Wells Fargo & Co*، ومصرف *Bancorp*، وخدمات *PNC* المالية لضمان تأثير كبير والتحكم بعدد كبير من حواسب النظام وكياناتها السيبرانية.

وقد تسارعت وتيرة التطورات الحاصلة في تقنيات القرصنة، وإنتاج البرمجيات الخبيثة، والهيمنة على المرور السيبراني في فضاء الإنترنيت العولمي بحيث نجد أن *Eric Schmidt* عضو مجلس الإدارة في مؤسسة *Google* قد عبّر عن دهشته البالغة بالقدرات التي أضحى يتمتع بها قراصنة المعلومات الذين يعملون بمعية جيش فضاء السيبراني، ولم يجد تبريراً موضوعياً للتطور الكبير في قدراتهم عندما أعلن عن قيامهم بالهيمنة على المرور السيبراني في الإنترنيت المتجه الى الدانمارك بواسطة آلية قرصنة ذكية مغيرين اتجاهه نحو إيران، قبل أن يعيدوه ثانية باتجاه الدانمرك !(*BBC,2013*).

ولضمان تعمية ممارسات فصائل الحرس الثوري السيبرانية، وإخفاء بصمات حضورها السيبرانية، لإبعاد الشبهات عنها، فقد حرصت على إطلاق هجمات جيشها السيبراني من مضيفات خدمة تستقر خارج حدود إيران. وقد أكدت حزمة من التقارير الأمنية التي صدرت عن مراكز البحوث المتخصصة بملفات أمن الفضاء السيبراني أن جل التهديدات والهجمات التي مورست بواسطة جحافلها السيبرانية، خلال الأطوار الثلاثة للسجالات السيبرانية، قد انبثق فيض نبضاتها السيبرانية من مضيفات خدمة في باكستان، والصين والإمارات (*HP,2014,a*).

وكان لمجاميع قراصنة المعلومات الموالية للنظام، والتي عملت تحت راية مؤسسة الحرس الثوري الإيراني، أو مارست عملية التنسيق مع فصائله، دوراً لا يستهان به في السجالات السيبرانية التي حصلت خلال هذا التطور.

فقد قامت مجموعة قراصنة *Parastoo* بقرصنة مجموعة حواسب في المنظمة الدولية للطاقة الذرية *International Atomic Energy Agency (IAEA)* على التوازي مع حواسب أخرى في وزارة الطاقة الأمريكية *United States Department of Energy* خلال الربع الأخير من عام 2012 (*IICT,2013*).

وشأن الكثير من مجاميع قراصنة المعلومات في إيران فقد شرعت مجموعة *Ajax Team* بسلسلة هجمات على مواقع المعارضة الإيرانية، داخل حدود إيران وخارجها، بوصفه جزءاً من التزام المجموعة مع الحرس الثوري والنظام الإيراني بمناسبة ذكرى وفاة آية الله سعيد محمد حسيني بهشتي (*IICT,2013*).

ورغم حرص فريق قراصنة *Mortal Combat* على عدم الظهور في وسائل الإعلام الإيرانية، أو مواقع الويب، وإعراضه عن الإعلان عن هجماته السيبرانية المختلفة، بعد حضور في مجتمع قراصنة المعلومات دام أكثر من عقد من الزمن، إلا أن هناك الكثير من الأدلة التي تؤكد قيام هذا الفريق بصناعة الفايروس الخبيث *Mehdi Virus*[219] والذي نجح

[219] . تميز فايروس المهدي الذي ولد في تموز عام 2011 بامتلاكه قدرات تشابه الى حد كبير الفايروس الشهير *Flame* والتي تم الكشف عنها بعد أن عولجت آثار إصابته لأهداف رقمية في إسرائيل، ودول متعددة في الخليج العربي. لقد أظهرت عملية تشريح الخوارزمية لهذا الفايروس قدرته على مهاجمة الأهداف واستلاب بيانات مهمة من قواعد بياناتها (*OB,2013*).

باستهداف الكثير من الأهداف الصهيونية بآثاره الضارة والوخيمة كرد فعل على هجمة الفايروس الخبيث *Stuxnet*(*IICT,2013*).

وبدأنا نلحظ تطوراً في الهجمات السيبرانية التي اكتسحت مواقعاً متنوعة في الفضاء السيبراني الإسرائيلي، وفي مفاصل أوجعت الكيان الصهيوني.

فقد كشفت كوادر الأمن السيبراني في مصرف حابواليم *Hapoalim* الإسرائيلي في شهر فبراير من عام 2012 عن نشوب هجمة معلوماتية من إحدى مضيفات الخدمة الإيرانية (ومن خلال توظيف عنونة مواقع إنترنيت كندية) عمد أصحابها الى زرع دودة خبيثة بواسطة ملف[220] أرسل الى مجموعة موظفين في هذا المصرف. وقد صممت هذه الدودة الخبيثة لاستراق البيانات المصرفية الشخصية لزبائن المصرف وتسريبها الى إيران لصالح جهة معينة، بيد أن الفريق الأمني قد نجح في الكشف عن وجود الدودة، حال محاولة تسللها وقام بحظر نشاطها قبل أن تشرع في مهمتها السيبرانية (*Even&Siman-Tov,2012*).

ومع إطلالة عام 2013 قامت مجاميع من قراصنة المعلومات الإيرانيين بهجمات نوعية استخدمت آليات رفض الخدمة وتضليل نظام نطاق التسمية في نظم المعلومات الصهيونية رداً على العملية التي وجهها الكيان الصهيوني على قطاع غزة وأطلق عليها عملية أركان الدفاع *Operation Pillar of Defense* في عام 2012. أقرّ الخبراء الصهاينة بتطور القدرات الهجومية ـ الإيرانية في تنفيذ هذه الهجمات، وأن فصائلها السيبرانية باتت قادرة على ممارسة سلسلة من الهجمات، وبمستويات تهديد متعددة، وعلى أهداف متنوعة، بالوقت ذاته (*INSS, 2014*).

ولم يتغيب القراصنة الذين يدفعهم حس الانتماء الوطني لإيران من ممارسة دورهم في السجال السيبراني الدائر في هذا الطور. فقد أشارت بعض التقارير الى الكشف عن وجود هجمات ضد مواقع إسرائيلية متنوعة بدأت عام 2013، دون أن تتوفر دلائل واضحة حول ارتباطها المباشر بجيش إيران السيبراني *ICA*وظفّت فيها أدوات بدائية عند ممارسة الهجمات مما يؤشر نحو عمليات قرصنة تتوجه نحو ممارسة هجمات لصالح إيران بدافع الحس الوطني، أو مناهضة أعداء الأمة، بعيداً عن وجود دعم مباشر من قبل النظام لهؤلاء القراصنة السيبرانيين (*ICIT,2015*).

ولم تقتصر ممارسات السجال السيبراني على الدفاع عن الحياض السيبرانية لإيران، بل امتدت لتعبّر عن مناهضة الهجمات الإسرائيلية ضد قطاع غزة، حيث تستوطن كتاب القسام السيبرانية، الموالية للنظام الإيراني. ونتلمس هذا عندما نطالع تفاصيل الهجمة التي أمطرت بها هذه الفصائل لعدد كبير من المواقع الإسرائيلية للتعبير عن شجبها للهجمة الإسرائيلية الشرسة على قطاع غزة والتي أطلق عليها عملية *Operation Protective Edge* في عام 2013 (*Siboni& Kronenfeld,2014*).

وخلال سنة 2013 باشرت مجموعة من مقاتلي القسام السيبرانيين بسلسلة من الهجمات السيبرانية ضد أهداف منتخبة في القطاع المالي والمصرفي بالولايات المتحدة الأمريكية خلال شهر سبتمبر من عام 2013، شملت كل من: *Bank of America Corp, J.P. Morgan, Chase, U.S. Bancorp, PNC Financial Services Corp., Wells Fargo & Co, Capital One, Sun Trust Banks Inc., & Regions Financial Corp.* بواسطة آلية هجمات

[220] . الملف هو لعرض تصميمي أعد بواسطة التطبيق الشائع *Microsoft Power Point*.

رفض الخدمة، والتي نشب عنها حصول تباطؤ ملحوظ في أداء بعض مواقع ويب وتوقف أخرى عن العمل بصورة مؤقتة بهذه المؤسسات المالية المرموقة. وقد تبين من تحليل آثار هذه الهجمات ومسارات انطلاقها أنها قد تمت تحت هذا الغطاء لصرف النظر عن مساهمة أكثر من 100 مجموعة قراصنة وقراصنة معلومات متطوعين[221]، ينتمون الى مؤسسات أكاديمية إيرانية، تطوعوا لممارسة هذه الهجمة الشرسة بالإنابة عن النظام الإيراني (*Schwarz,2013*).

وامتد نطاق الهجمات التي أغار بها خصوم إيران على مشروعها النووي ومؤسساتها الحيوية بواسطة الفايروسات والبرمجيات الخبيثة، التي طارت شهرتها بالآفاق، وتوسعت ساحة السجالات السيبرانية فحفلت بهجمات متنوعة، بعضها نشأ من الولايات المتحدة، أو إسرائيل، أو من دول منطقة الشرق الأوسط، مستهدفة كيانات رقمية مختلفة، وبمستويات تأثير متباينة.

ولا يمكن الإحاطة بتفاصيل هذه الهجمات، لكثرتها وتباين مساراتها، الأمر الذي أجبرنا على انتخاب أهم الهجمات المؤثرة في هذه المرحلة، ومنها قيام مجموعة من القراصنة الذين يناصرون إسرائيل، أطلقوا على أنفسهم لقب "فريق وزارة الدفاع الإسرائيلية *IDF Team*" في بدايات عام 2012 بمهاجمة موقع صحافة التلفزيون الإيراني، وموقعين آخر يعود الى وزارة الصحة والتعليم الصحي في الجمهورية الإسلامية فأحدثت خللاً فيهما (*Even&Siman-Tov,2012*).

ولم تمر سوى مدة يسيرة حتى أعلن أحد المسؤولين في وزارة النفط الإيرانية *Iranian Oil Ministry* (في النصف الأول من السنة ذاتها) عن حصول هجمة معلوماتية خطيرة نشب عنها إصابة منظومة إدارة عمليات تصدير النفط الإيراني (الموجودة في جزيرة خرج) بواسطة برنامج خبيث مما اضطر الإدارة الحكومية الى اتخاذ قرار فوري بوقف تشغيل هذا النظام بصورة مؤقتة لحين معالجة آثار الإصابة واحتواء تأثيراتها[222]. وقد عاد الناطق بلسان الوزارة فأكد عدم حصول خلل في بيانات المنظومة، كما أن هذه الآفة لم تفلح بالتسلل الى منظومة المعلومات الإيرانية ـ الوطنية نتيجة اعتماد مبدأ عزل هذه المنظومة عن نسيج المعلومات الوطني ومضيفاته الأساسية (*Jackson,2012,c*).

من جهة أخرى، ذكر الجنرال غلام رضا جليلي، قائد مؤسسة الدفاع المدني الإيراني، خلال مقابلة صحفية مع وكالة مهر الإخبارية عن اكتشاف بصمة لبرنامج خبيث أصاب منظومة المعلومات الحكومية ـ الإيرانية. ولم تنشب عن هذه الإصابة تأثيرات ضارة ملموسة[223]، أطلق عليه فايروس *Star*. وقد أقر جليلي أن خبراء أمن المعلومات لم يفلحوا في كشف اللثام عن جميع تفاصيل خوارزمية معماريته البرمجية، الأمر الذي يشكل عقبة أمام عملية استشراف مستقبل تأثيراته المحتملة على نظم المعلومات الإيرانية. من أجل هذا ذهبت بعض الشركات المتخصصة في مكافحة البرمجيات الخبيثة الى اعتباره نسلاً جديداً نشأ عن الإصابة بفايروس *Stuxnet* الذي طال المنشآت النووية الإيرانية (*Schwartz,2011*).

---

[221] . كان حجم التهديدات المصاحبة لهذه الهجمات كبيراً، بحسب تقرير التقرير الذي أعده مركز حماية أمن المعلومات في إسرائيل، مع بروز بينات واضحة لقيام هذه الفرق بتوظيف تقنيات قرصنة متقدمة لا يمكن أن تقوم بها جهة واحدة، بل مجموعة من فرق القرصنة السيبرانية، وبتوفر دعم لوجستي، وبنية تحتية للمعلومات قادرة على توفير مستلزمات إنجاح مثل هذه الهجمة الشرسة.

[222] . بعد مدة قصيرة، أفصحت مؤسسة مهر الإخبارية ـ الإيرانية عن امتداد آثار هذه الهجمة واصابتها لكثير من الحواسب في وزارة النفط الإيرانية، بالإضافة الى حواسب أخرى في الشركة الإيرانية ـ الوطنية للنفط *National Iranian Oil Company* (*Jackson,2012,c*).

[223] . لوحظ أن الفايروس قد أصاب ملفات برمجيات معالجة النصوص مثل: *Word, Excel, PDF* .

ولم يخل فضاء السجال السيبراني من هجمات ذات منطلق عقدي، مورست بواسطة قراصنة معلومات ينتمون الى صبغة عقدية تختلف عن الصبغة الإيرانية، فقد أعلن موقع حنين الذي ينتمي الى أحد المنتديات الجهادية، قيام مجموعة من قراصنة المعلومات الملتحقين به في شن هجمات على أكثر من 100 موقع إيراني يروّج ممارسة زواج المتعة المنهيِ عنه في المدونات الفقهية لأهل السنة والجماعة (*Azani,2015*).

5 . 3 . 3 . السجالات السيبرانية بعد هجمة الفايروس *Stuxnet* وولادة الأجيال المستنسلة عنه:

بعد أن نجح فايروس Stuxnet بالوصول الى أهدافه المرسومة، وحقق غاياته في خلخلة عمل أجهزة الطرد المركزي في المشروع النووي الإيراني بموقع نطنز، مما نشب عنه تأخير كبير في توقيتات المشروع، ثم بدأت الولادات المتتالية لأنساله مثل الفايروس الخبيث Flame، و Duqu وغيرهما من البرمجيات الخبيثة، وجدت الإدارة الإيرانية أن حجم الأخطار السيبرانية التي تحدق بالبلاد باتت تشكّل تهديداً جسيماً لكياناتها، وبرامجها التنموية في شتى المجالات، بالإضافة الى التهديدات المستمرة من خلال الهجمات اللينة التي لم تنقطع منذ أكثر من عقد من الزمان. فلم تجد مناصاً من تطوير قدرات الردع السيبراني لديها الى مستوى يرقى بها الى مستوى متقدم على صعيد السطوة السيبرانية لكف هجمات خصومها.

وأسهم حجم التحدي غير المسبوق الذي تعرض له الفضاء السيبراني الإيراني، والكيانات السيبرانية المرتبطة به (منشآت نووية، ومؤسسات حكومية حساسة، والبنية التحتية للمعلومات والاتصالات) وخلال بعد زمني قصير، في اقتناع الإدارة الحكومية بضرورة وجود مستوى عال من التنسيق بين جميع القطاعات لإرساء قواعد متينة لجدار رقمي قادر على صد مثل هذه الهجمات، أو التقليل من آثارها المحتملة، بالإضافة الى التفكير في استخدام الاستراتيجية الهجومية لكف هجمات خصومها. ولا بد من التنويه الى أن هذه المهام الخطيرة مجتمعة لم تصرف النظام الإيراني عن تركيز الاهتمام على المعارضة وحضورها السيبراني في فضاء إيران السيبراني، فسخّرت له جزءاً لا بأس به من اهتمامها الذي عبّرت عن بسلسلة تهديدات وهجمات معلوماتية لكفّ نشاط المعارضة وتكميم أفواه كياناتها.

وبدأت الإدارات السيبرانية ـ الايرانية، في الوقت ذاته، بتثوير تربة القرصنة السيبرانية والتوجه نحو صنع برمجيات خبيثة تمتلك القدرة على ممارسة عمليات تخريبية واسعة في البنى التحتية للمعلومات والاتصالات، وتملك بنية برمجية معقدة تدعم عمليات التسلل داخل عقد النسيج الشبكاتي لنظم معلومات خصومها وممارسة سلسلة عمليات جمع واستقصاء بيانات تدعم أنشطتها الأمنية والاستخبارية، وتوفر، بالوقت ذاته، بيانات تقنية من قواعد البيانات والمستودعات السيبرانية لبيوت الخبرة العالمية، يمكن أن تستثمر في تحريك عجلة التنمية التقنية بإيران وتطويرها.

ورغم تكاثر هذه المهام وتشابكها، مع تزايد عديد الهجمات، وعمق التهديدات والمخاطر المصاحبة لها، لم تفقد الإدارة الإيرانية هدوءها المعهود في التعامل مع المسائل الحرجة، فحرصت على إبعاد الشبهات عن دائرة ممارساتها السياسية، وحاولت تشتيت الانتباه، وتغييب أي بصمة يمكن أن توظف لكيل الاتهامات للنظام ومؤسساته الأمنية.

فلقد ضمن النظام الإيراني حصول تغير ذوعي ومزلزل في استراتيجية البلاد السيبرانية والتي تحوّلت تدريجياً من النزعة الدفاعية باتجاه نزعة هجومية شرسة (*Berman,2013*) نجحت من خلالها بمهاجمة الكيانات السيبرانية لخصومها

بكل ما أوتيت من سطوة رقمية، مع حرص محموم على تطوير قدرة آلتها السيبرانية لكي تضمن التربع على مرتبة متقدمة في مضمار السطوة السيبرانية والتفوق السيبراني (*Jackson,2012,a*).

وقد أفصح غلام رضا جليلي، رئيس مؤسسة الدفاع المدني الإيراني، عن الدور المهم الذي مارسته هجمة الفايروس الخبيث *Stuxnet* والتي عززت نهج متماسك من التنسيق المشترك بين جميع المؤسسات الأمنية في إيران، وبحضور مكثف لمؤسسته ووزارة المخابرات الإيرانية، ومؤسسة الحرس الثوري الإيراني، والهيئات القضائية لتسخير جميع الإمكانيات المتاحة بالبلاد للارتقاء بالكفاية الأمنية لالفضاء السيبراني الإيراني، وترسيخ حصانته ضد أية هجمات محتملة بالمستقبل القريب (*MAI,2011*).

ولم تقتصر التطورات على هذه المحاور بعد أن عزز عزز النشاط السيبراني الإيراني عن طريق تبني نهج استبطن منطقاً بالغ التعقيد، انتقى بعناية أساليب ممارسة الهجمات، ومواردها، وأدواتها بحيث يتحقق الحد الأقصى من غايات عمليات التلصص، أو التهديدات، أو الهجمات السيبرانية بمختلف أنماطها، مع تغييب أي علامة أو إشارة يمكن أن تستثمر لتوجيه إصبع الاتهام نحوه أو نحو مؤسسة الحرس الثوري الإيراني.

ويمكن تأكيد ما ذهبنا إليه من مراجعة التقرير الذي أعده المعهد الأمريكي تحت مظلة مشروع التهديدات الحرجة وبالتنسيق مع مؤسسة *Norse* (التي ترعى مشروع تتبع مصادر جميع أشكال التهديدات والهجمات السيبرانية التي تنشأ عن الفضاء السيبراني الإيراني) عن جزء يسير من هذا النهج المعقد، والذي بات يستنزف الكثير من جهود خبراء أمن المعلومات الغربيين، ويشتت انتباههم بين مصادر متعددة للتهديدات والهجمات، والتطور السريع في عمليات تنفيذها، وتقاصر المدد الزمنية التي تستغرقها هذه الهجمات (*Kagan&Stiansen,2015*).

فلقد لوحظ أن جلّ الهجمات التي تنطلق من فضاء إيران السيبراني تنشأ عن نظم شبكات الحواسب المقيمة لدى مؤسسة الحرس الثوري الإيراني، وبواسطة تقنيات بالغة التعقيد، في سعي حثيث لتفحص أنماط حضور المئات من الكيانات السيبرانية بالولايات المتحدة ودول أخرى مناوئة، عبر مضيفات خدمة تقيم في إيران، وخلال بعد زمني لا يتجاوز بضعة ثوان. ولولا المراقبة المستديمة التي تحرص عليها مؤسسة *Norse* لضاعت هذه النبضات اللحظية في زحمة المرور السيبراني الكوني في فضاء الإنترنيت. كذلك تمارس عمليات تفحّص مشابهة بواسطة مضيفات جامعة شريف للتقنية للعثور على الثغرات الأمنية بنظم المعلومات المنتشرة في النسيج الشبكاتي للولايات المتحدة، وخلال البعد الزمني ذاته.

لقد حفل هذا التطور بكم كبير من أنشطة السجال السيبراني بين إيران وخصومها داخل إيران، وخارج حدود فضائها السيبراني ـ الوطني، مع تطور النزعة لدى الأطراف المتخاصمة لإحداث تأثيرات مؤذية، وعميقة لدى الطرف الآخر.

وإذا حاولنا البدء من ساحة خصوم إيران سنجد أن عملية الاستنسال من البصمة الجينية للفايروس الخبيث *Stuxnet* قد استمرت ضمن هذه الحقبة، والتي أثمرت عن ولادة برمجيات أشدّ خبثاً وتأثيراً على الكيانات السيبرانية المقيمة في فضاء إيران السيبراني.

ففي عام 2012 أعلنت شركة *Symantec* (المتخصصة في مكافحة البرمجيات الخبيثة) عن عثورها على بصمة برنامج خبيث جديد ينزع نحو مهاجمة الأهداف المالية والمصرفية يحمل اسم *Narilam* ويتميز بمعمارية برمجية معقدة

تمنحه القدرة على ممارسة هجمات مؤثرة على مؤسسات مالية ومصرفية من خلال إحداث خلل في نظم الملفات الموجودة بالحواسب، عن طريق إلغاء أجزاء منتخبة منها (*Schwartz,2012,a*).

وحال إصابة الحواسب بالآفة، يباشر البرنامج الخبيث باستنساخ لبابه ويبدأ بالانتشار الى حواسب أخرى عن طريق إصابة المشغلات المتحركة *Removable Drives*، أو مشاركة البيانات عبر نظام الشبكات المحلية، فيستمر بعملية التخريب وخلخلة نظم الإدارة المالية في المؤسسات المصرفية.

وبعد صدور التحذير عن شركة *Symantec* هرع مركز *MAHER* الإيراني الى الإعلان عن إصابة هذا البرنامج الخبيث لمجموعة من المؤسسات المالية الإيرانية، وذكر أن كوادره قد نجحت في احتواء آثار هذه الآفة بسرعة دون حدوث تأثيرات ضارة بهذه النظم (*Schwartz,2012,a*).

وشهد عام 2014 ولادة جيل جديد من سلالات الفايروس الخبيث *Stuxnet* تمت عملية تطويره تحت إشراف مجموعة من قراصنة المعلومات المتمرسين، وأطلق عليه اسم *Regin*. وتألفت معمارية هذا البرنامج الخبيث من مجموعة عناصر توجه مساراتها خوارزمية بالغة التعقيد، استهدف أصحابها توظيف أساليب خفية، ونظم ملفات افتراضية ـ مشفّرة لجمع بيانات ومعلومات مهمة عن طريق المراقبة المستمرة لأنشطة أفراد محددين، ومؤسسات تمتلك أهمية استراتيجية في إيران(*HP,2015*).

ومع تزايد حجم التجاذبات السياسية بين المملكة العربية السعودية والنظام الإيراني منذ عام 2015 وامتدادها الى عام 2016 تكاثرت الهجمات السيبرانية المتبادلة بين قراصنة المعلومات الموالين لهذا المعسكر وذاك. ولعل من الهجمات التي أثارت سخط النظام الإيراني هي تلك التي قام بها قرصان سعودي أطلق على نفسه *Crazy-3r3r* الذي نجح باختراق موقع التدوين الرسمي لبوابة الويب المخصصة للإمام الخميني وأقحم بالموقع صورة لطائرة مقاتلة إيرانية تحمل في مخالبها قائد الثورة الإسلامية (*Waqas,2016*).

أما إذا أردنا التوجه صوب الكشف عن طبيعة أهم الهجمات التي مارستها الفصائل السيبرانية الإيرانية (بجميع انتماءاتها) ضد خصومها في الفضاء العولمي ـ السيبراني، فسنجد أنفسنا قبالة كم كبير من التهديدات والهجمات المتنوعة التي تباينت آلياتها، وتنوعت جغرافية أهدافها، وتعددت هويات المساهمين بشنّها على مستوى الأفراد، والفصائل السيبرانية الإيرانية.

فنبدأ بسلسلة هجمات من نوع *Newscaster* ضد إسرائيل، والولايات المتحدة، ودول متعددة في أوربا، كشفت تحريات مؤسسات الأمن السيبراني الإسرائيلي عن قيام إيران بشنها عام 2011 لجمع بيانات استخبارية والترويج لهويات رقمية منتحلة ترتبط مع مؤسسات حكومية، أو كيانات صحفية. ولم يتم الكشف عن هذه الهجمات حتى عام 2014 بعدما عثر على بصماتها في أكثر من 2,000 حاسب متوزع بين هذه البلدان (*Cohen,et.,al.,2015*).

وتميز عام 2012 بهجمة قام فريق من القراصنة الإيرانيين أطلق على نفسه اسم "سيف العدالة القاطع *Cutting Sword of Justice* في شهر أغسطس من عام 2012 وذلك عن طريق إقحام فايروس خبيث أطلق عليه اسم *Shamoon* في شبكة المعلومات الداخلية لشركة أرامكو السعودية ـ النفطية (*Cilluffom,2013*)، والذي باشر على الفور نشاطه التخريبي الذي شمل إلغاء بيانات مهمة في أكثر من 30,000 حاسب من حواسيب الشركة، بالإضافة الى إدراج صورة لعلم الولايات المتحدة الأمريكية الذي التهمته النيران. ولم تمر سوى مدة يسيرة حتى مورست هجمة

شرسة على شركة *RasGas* التي تعمل في قطاع تسييل الغاز الطبيعي في دولة قطر، وأحدثت فيها أضراراً مشابهة (*OB,2013*). وفي العام ذاته، أعلنت مجموعة من القراصنة الإيرانيين التي تطلق على نفسها اسم *Iran Cyber Warriors Team* عن نجاح سلسلة الهجمات التي قامت بها على حسابات بضعة آلاف من الأشخاص العاملين في مؤسسة الفضاء الأمريكية *NASA* باستخدام آلية الشخص الوسيط *'Man In The Middle'* (*Jackson,2012*).

ويعد توظيف هذا النوع من الهجمات من التهديدات الخطيرة، وبعيدة المدى، ذلك أن الهجمة لا تستهدف إحداث تأثيرات ملموسة وإنما ترسّخ للجهة المهاجمة حضوراً وسيطاً بين المستعرضات ومؤسسة *NASA*، أو داخل البنية البرمجية أو معدات الجدران النارية التي تستخدمها المؤسسة مما يشكل تهديداً دائماً لهذه المؤسسة الاستراتيجية (*Jackson,2012*).

وقد ذهب الكثير من خبراء أمن المعلومات والمتخصصين بتحليل آثار التهديدات والهجمات السيبرانية الى اعتبار الهجمة التي مارسها الفايروس *Shamoon* من أكثر الهجمات التي مورست دفعة واحدة وعلى شركة منفردة. وتعد الهجمة التي مارسها هذا الفايروس، في أسلوبها، بعيدة عن النهج الذي اتسم به فايروس *Stuxnet*، حيث توجهت مسارات الهجمة نحو الحواسب دون أن تحدث خللاً في نظم المعلومات الموجودة بشركة *Aramco* السعودية، وكان الهدف الرئيسي من نشاطه إحداث تدمير شامل في البيانات الموجودة بالحواسب مع إحداث خلل كلي في أدائها. بيد أن من الجدير بالذكر هو احتواء المعمارية المنطقية للبرنامج على شيفرة[224] *Word Wiper* والتي كانت موجودة في برنامج *Flame* الذي يعد من الجيل الثاني لبرنامج *Stuxnet* (*Siboni&Kronenfeld ,2014*).

وشهد عام 2013 (هجمة أخرى لفصائل القرصنة السيبرانية الإيرانية) عدّها المتخصصون في مجال الأمن السيبراني نقطة تحوّل كبير في نهج الهجمات الإيرانية ضد أهداف منتخبة بالولايات المتحدة، ودول أخرى عندما نجحت مجموعة تتألف من سبع قراصنة في ممارسة سلسلة من الهجمات السيبرانية طالت منظومة إدارة إحدى السدود الأمريكية، ومجموعة من المؤسسات المالية الأمريكية، بين شهري أغسطس وسبتمبر من عام 2013 بالتنسيق مع فريق قراصنة المعلومات *ITSecTeam* (*ITSEC*) وشركة *Mersad Company* (*MERSAD*) واللتان تعملان مع مؤسسة الحرس الثوري الإيراني (*Grobman,2016*).

وقد هرعت وزارة العدل الأمريكية *DoJ* بتوجيه التهم الى سبعة من قراصنة المعلومات الإيرانيين، والتي عدتها تهديداً سافراً للأمن القومي في الولايات المتحدة.

وقد تنصل النظام الإيراني ونفى أي صلة له بمثل هذه العملية بتصريح للناطق بلسان الخارجية الإيرانية، جابري أنصاري، حيث نفى الاتهامات التي وجهتها وزارة العدل الأمريكية (ضد مجموعة من قراصنة المعلومات الإيرانيين وقيامهم بسلسلة هجمات ضد إحدى منظومات إدارة السدود الأمريكية، وهجمات متفرقة ضد مؤسسات مالية ومصرفية بالولايات المتحدة) وعدها اتهامات باطلة تفتقر الى أدلة قاطعة تثبت مثل هذه التهم. وأكد في تصريحه أن الحكومة الإيرانية ومؤسساتها لا تمارس أي نشاط يهدد الغير في الفضاء السيبراني، كما أنها لم تدرج في أجندتها أية أهداف لشن هجمات معلوماتية ضد الولايات المتحدة، وغيرها من الدول رغم كونها تناصب حكومته العداء

[224] . استدل من وجود هذه الشيفرة في المعمارية البرمجية لهذا الفايروس على ضلوع إيران بهذه الهجمة حيث قد استثمرت كوادرها السيبرانية وجود هذه الشيفرة في الفايروس الذي أصاب نظمها البرمجية وأعادت توظيفه في خوارزمية الفايروس *Shamoon* الذي استهدفت به المنشآت النفطية السعودية والقطرية.

(*Grobman,2016*). ولم تمر سوى مدة قصيرة حتى شنّ قراصنة معلومات (ينتمون الى إيران) سلسلة هجمات على كازينو *Sands Casino* في مدينة لاس فيجاس ونجحوا بسرقة بيانات مهمة من منظومة إدارة عمل الكازينو، وشلّ عملها لمدة ليست بالقصيرة. وقد مورست الهجمة للانتقام من الملياردير *Sheldon Adelson* الذي يمتلك الكازينو كرد حاسم على تصريحات معادية لإيران[225] سبق وأن أطلقها في عام 2013 (*Luce,2015*).

من جهته، ذكر بيروز كماليان أن مجموعة قراصنة *Ashiyane* قد اخترقت مجموعة مواقع بمنطقة الخليج العربي للتعبير عن رفضها لاستخدام عبارة الخليج العربي بدلاً من الخليج الفارسي وأقحمت فيها التسمية الأخيرة. شملت هذه المواقع، مواقع ويب في: السعودية، والإمارات، والبحرين، وعمان، والعراق (*Mansharof,2013*).

ولم تقتصر هجمات هذه المجموعة على مواقع المعارضة الإيرانية، المقيمة داخل إيران وخارجها، بل امتدت ذراعها السيبرانية الى مواقع تقيم في فضاء المملكة العربية السعودية فنجحت خلال شهر مارس 2013 بصولة على موقع *Mef.edu.sa* الذي ينتمي الى مواقع وزارة التعليم العالي بالمملكة، وأورثته خللاً تقنياً، ثم لم تلبث أن باشرت بسلسلة هجمات على مواقع تعود لمؤسسات حكومية سعودية منتخبة خلال شهر يونيو من العام ذاته تعبيراً عن سخطها بسبب دعم المملكة المستمر للبحرين في قمع المعارضة الشيعية (*Mansharof,2013*).

أما عام 2014 فقد كان حافلاً بسلسلة من التهديدات والهجمات الإيرانية، وعلى نطاق جغرافي واسع. (إحداها) عندما شنّ قرصان معلومات إيراني (أطلق على نفسه اسم *Mr.XHat*) هجمة شرسة على نطاق تسجيل المضيفات في طاجكستان، في 6 يناير من عام 2014، نجحت في إيقاف عمل الكثير من المواقع والتطبيقات، مثل *Google, Twitter,Yahoo, Amazon* لمدة يوم تقريباً. وقد أودع القرصان رسالة تهديد باللغة التركية ليوهم الإدارة السيبرانية في طاجكستان ويشتت انتباههم عن موطنه إيران (*IICT,2014*).

و(الثانية) عندما أعلنت مجموعة قراصنة المعلومات الإيرانيين *Parastoo* عن مشاركتها في الهجمة الشرسة على الفضاء السيبراني الإسرائيلي، والتي أطلق عليها اسم عملية معارضة ولادة إسرائيل *“OpIsrael2 (Op Israel Birthday)”* وبالتنسيق مع مجاميع إيرانية أخرى، منها جيش فضاء إيران السيبراني، ومجموعة أبابيل، ومجموعة المقاومة الإسلامية، والفصائل السيبرانية لحزب الله اللبناني (*IICT,2014*)، كذلك، قام قراصنة معلومات إيرانيون باختراق حسابات موظفين في وزارة الخارجية الأمريكية عن طريق استراق حساباتهم في تطبيقات منصة شبكات التواصل الاجتماعي في نهاية شهر نوفمبر من عام 2014. استهدفت هذه الهجمات مجموعة من الموظفين الذين يتابعون شؤون إيران، ودول مختلفة بالشرق الأوسط، في محاولة للتجسس على أنشطتهم واستراق بيانات ذات صلة بنهج تعامل الإدارة الأمريكية مع هذه البلدان (*Snapshots,2015*).

ـ أنظر كذلك الجدول (6- 2).

[225] . قال في إحدى تصريحاته أمام الرأي العام الأمريكي " ينبغي توجيه ضربة لإيران *Iran should be nuked*".

الجدول (6 - 2) ـ سجل بأهم الهجمات التي شنتها الفصائل السيبرانية الإيرانية على أهداف منتخبة في فضاء الفيض السيبراني.

الجهة التي مارست الهجمات	أهم الأهداف التي شنّت عليها الهجمات
جيش فضاء إيران السيبراني.	موقع *Twitter*، آلة البحث الصينية *Baidu*، موقع صوت أمريكا *VOA*، اختراق موقع منظمة حقوق الإنسان بالولايات المتحدة.
مجموعة قراصنة Ashiyane.	موقع قائد الموساد ووزير الدفاع الإسرائيلي باراك، موقع وكالة الفضاء الأمريكية *NASA*، اختراق سجل نطاق دولة طاجكستان، اختراق النطاق الإسرائيلي il، اختراق مواقع حكومية لكل من: إندونيسيا، والهند، والصين، وتايلاند، والأرجنتين، وبنغلاديش، وتركيا، واختراق موقع ولاية أوريغون بالولايات المتحدة.
مجموعة المقاومة الإسلامية لالفضاء السيبراني.	موقع شركة أرامكو السعودية، موقع شركة الاتصالات *Zain*، موقع وكالة الفضاء الأمريكية *NASA*، موقع وزارة الدفاع الإسرائيلية، مجموعة بن لادن السعودية، المشاركة في الحملة المناوئة للبحرين *#OpBahrain* وتسريب معلومات مهمة من وزارة الدفاع البحرينية، والحملة المناوئة للهجمات الصهيونية على قطاع غزة *#OpIsrael*.
مجموعة قراصنة Parasto.	عملية *#OpIsrael*، موقع الوكالة الدولية للطاقة الذرية، موقع *HIS Jane's Defense*، قرصنة طائرة أمريكية مسيّرة.
مجموعة قراصنة Ajax Team.	هجمة على موقع وكالة الفضاء الأمريكية *NASA*، هجمة على موقع جامعة كولومبيا بالولايات المتحدة.

المصدر: *HP,2014, 2014a*.

كذلك لم يخلو العامين 2015-2016 من هجمات للفصائل والمجاميع ذاتها على أهداف منتخبة، منها: مجموعة من الهجمات الشرسة على أكثر من إدارة تعنى بإنتاج الطاقة الكهربائية في إسرائيل، وأخرى اخترقت الجدار الأمني واستهدفت مضيف الخدمة بمصرف أورشليم واستطاعت الحصول على البيانات الشخصية لبضعة آلاف من زبائنه، وثالثة شنت على مواقع قيادات رفيعة في جيش الدفاع الإسرائيلي، ونجحت بالحصول على معلومات حساسة. ورابعة، عن طريق شنّ حملة على موقع تواصل الشبكة الاحترافية *LinkedIn* عن طريق إنشاء شبكة رقمية موازية ـ مزيفة (خلال شهر أغسطس عام 2015) نجحت من خلالها استدراج عدد كبير من المتخصصين والخبراء يعملون في القطاع الحكومي، وآخرين يعملون في شركات تتعامل مع قطاع الدفاع في منطقة الشرق الأوسط، وشمال أفريقيا، وذلك

بقصد الحصول على بياناتهم الشخصية، والتسلل الى مواقعهم للكشف عن طبيعة الأنشطة التي يمارسونها في بلدان هذه المناطق. وهجمة خامسة أطلق عليها *Oil.Rig* شنّت على مؤسسات نفطية وأخرى مالية في المملكة العربية السعودية، وخامسة استهدفت مؤسسات وشركات مرتبطة بوزارة الدفاع الأمريكية، البنتاغون[226].

أما على صعيد السجال السيبراني الإيراني داخل حدود فضاء إيران السياسي، فقد استمرت مجاميع قراصنة المعلومات بالتنسيق مع مؤسسة الحرس الثوري الإيراني، عبر قناة جيش إيران السيبراني، والتواصل مع مؤسسة الباسيج في الكشف عن موارد التهديدات التي تنشأ عن حضور المعارضة التي تروم ممارسة هجمات معلوماتية في الفضاء السيبراني، لتمارس سلسلة من الهجمات بقصد الكشف عن هوية المعارضين، أو إحداث خلل في مواقع الجهات المناوئة للنظام (*Schwarz,2013*).

وفي شهر فبراير من عام 2013 قامت مجموعة الجهاد الافتراضية ـ المستقلة *Virtual Anonymous Jihad* باجتياح وإيقاف موقعين يرتبطان بصورة مباشرة مع الرئيس الإيراني السابق والمعارض للنظام الإيراني (المقيم في فرنسا) أبو الحسن بن صدر (*Enghelabe-eslami.com& Banisadr.org*). وعاودت المجموعة باكتساح موقع لقناة تلفزيونية *Irtv.com* بالولايات المتحدة، تعود للمعارضة الإيرانية خلال شهر أيار من العام ذاته، ثم باشرت هجمات متعددة في شهر يونيو، وقبيل بدء الانتخابات الرئاسية بإيران، انقضّت فيها على مواقع (*Digraban.com,Khodnevis.org&Ostanban.com*) والتي استضيفت خارج حدود إيران، وتعود الى شخصيات تعارض النظام الإيراني، وأوقفتها عن العمل، مع إيداع رسالة تحذيرية تنبه المعارضين الى عدم قدرتهم على الإفلات من قبضة حزب الله الإيراني حيثما حلوا وارتحلوا (*Mansharof,2013*).

وقامت مجموعتان من قراصنة المعلومات الإيرانيين هما *Cadelle and Chafer* (خلال عام 2014) قامت بالتجسس على مجموعة من المواطنين الإيرانيين، ومؤسسات تعود الى قطاعي الطيران والاتصالات في دول الشرق الأوسط باستخدام تقنية *Backdoor* (*Symantec,2015*) كذلك، أجهز القراصنة على موقع اتحاد الطلبة الإصلاحيين في جامعة أمير أكبر للتقنية، وموقع المسار الأخضر *Rah-e Sabz* الذي يدعم النهج الإصلاحي للمعارض مير حسين موسوي (*Zimmt,2010*).

أما أثناء حملة الانتخابات الرئاسية لعام 2013 فقد شن جيش فضاء إيران السيبراني بضعة عشر هجمة على مواقع المعارضة الإيرانية التي تعمل في فضاء إيران السيبراني، مثل: موقع صوت الأهواز، وموقع أهواز الحرة، وموقع المعارضة الانفصالية بالأهواز، ومدونة الصحفي الإيراني آراش سيكارجي، وموقع إيران العولمي، ومواقع أخرى تدار بواسطة المعارضة داخل إيران أو خارجها (*Mansharof,2013*).

ويضاف الى ذلك التحالف المتين بين من وزارة المخابرات الإيرانية (*Ministry of Intelligence (MOI*) والحرس الثوري الإيراني بالاشتراك في مهمة السجال السيبراني مع المعارضة الإيرانية في داخل البلاد، وذلك عن طريق المراقبة المستمرة لخطاب التواصل الذي يسافر عبر قنوات الرسائل القصيرة في الهواتف المحمولة، والتنصت على المكالمات الهاتف، أو استخدام أدوات وبرمجيات التلصص الإلكتروني على جميع قنوات التواصل السيبراني بين المواطنين الإيرانيين الذين

[226] . يمكن مراجعة تفاصيل هذه الهجمات، وهجمات أخرى لم نذكرها لضيق المقام في الموقع *http://www.hackmageddon.com/* الذي تعكف إدارته على إصدار تقارير نصف شهرية توثّق التهديدات والهجمات السيبرانية في فضاء الإنترنيت العولمي.

تحوم حولهم الشبهات لتوفير أدلة كافية للقبض عليهم وتطبيق قوانين الجرائم السيبرانية ـ الصارمة بحقهم (*FWC,2015*).

ولجأت هذه الجهات، في أحيان أخرى، الى توظيف مصائد إلكترونية للمعارضة الإيرانية عن طريق بث منشورات، أو تغريدات، أو صور، أو صناعة حسابات وهمية بأسماء قادة المعارضة وناشطيها المشهورين، بقصد استدراج البعض والإيقاع بهم. ويضاف الى كل ذلك وجود تطبيقات المراقبة والحظر الذكي الذي يمارس عملية الحظر والكف السيبراني على مادة المحتوى السيبراني الذي يعارض خطاب النظام الإيراني ليزيح هذه الخطابات من فضاء التواصل الإيراني ويحول دون انتشاره أو تداوله بصورة واسعة بين المستخدمين الإيرانيين.

ورغم الحرص الشديد الذي تبناه النظام الإيراني في التغطية على مساهمته الفاعلة بتغذية السجال السيبراني مع المعارضة بالداخل، وخصومه بالخارج فقد نجحت مجموعة شركة *HP* (المتخصصة بأمن المعلومات) في بتحديد هوية شبكة واسعة من قراصنة المعلومات الذين يوالون النظام الإيراني ويسعون الى نشر خطابه في فضاء الإنترنيت، ويحرصون على مدافعة حضور وهجمات خصومه، واستطاعت تحديد ملامح هذه المجاميع والقواسم المشتركة فيما بينهم، وهي: أن لغة خطابهم هي اللغة الفارسية، ويتأثرون جميعاً بخطاطة الثورة الإسلامية في إيران، ويعدّون الكيانات الغربية وإسرائيل أعداءً، ويشتركون باستخدام آليات تقنية وأخرى بدائية لاختراق أهدافهم السيبرانية، ويسعون الى إشهار تهديداتهم وهجماتهم من خلال قنوات شبكات التواصل الاجتماعي، أو موقع قرصنة المواقع الشهير *Zone-h*، كما أن قياداتهم تمتلك معرفة عميقة بممارسات القرصنة السيبرانية، وتربطهم صلات وثيقة، داخل حدود الفضاء السيبراني وخارجه، مما يذلل أمامهم عملية تنسيق الهجمات، وتوحيد أهداف هجماتهم (*HP,2014*).

5. 3. 4. السجالات السيبرانية لوكلاء إيران السيبرانيين:

لم تكتفي الإدارة الحكومية الإيرانية بتجنيد جلّ مؤسساتها، العسكرية والأمنية والمدنية، وشريحة واسعة من المواطنين الذين يمتلكون معرفة جيدة في القرصنة السيبرانية، وسبر مواطن الخلل في شبكات المعلومات للعمل معها وتوفير الدعم الكافي لإنجاح استراتيجيتها بشقيها الدفاعي والهجومي، ولكنها لجأت الى تجنيد قطعات رقمية، من خارج حدود البلاد، عن طريق تفويض وكلاء رقميين *Cyber Proxies* للتنسيق المباشر والعمل مع قواتها السيبرانية بتنفيذ مهام محددة ضمن الفضاء الافتراضي للدول المعادية للنظام الإيراني بعد أن رسّخ النظام الإيراني شراكاته وتحالفاته المتينة مع قراصنة المعلومات الإيرانيين توجه نحو توثيق صلاته مع قراصنة المعلومات المقيمين في الفضاء السيبراني العولمي، وخصص موارد مالية ضخمة لتمويل تهديدات وهجمات معلوماتية ضد أهداف منتخبة بالولايات المتحدة، أو توفير معلومات استخبارية عن مخططات أمريكية تخص ملف الأمن القومي الإيراني عن طريق تسريب بيانات من قواعد البيانات تقيم في مؤسسات حكومية بالولايات المتحدة[227].

[227] . عرضت شبكة *Univision Television Network* في شهر ديسمبر عام 2011 تحقيقاً متلفزاً أعلنت فيه عن حصول لقاء بين السفير الإيراني في المكسيك ومجموعة من قراصنة معلومات مكسيكيين، أبدوا استعدادهم لمباشرة سلسلة هجمات على أهداف منتخبة في البنتاجون، ووكالة المخابرات المركزية *CIA*، ومكتب التحقيقات الفيدرالية *FBI*، شريطة توفير الحكومة الإيرانية دعماً مالياً لهذا الفريق (*Siboni&Kronenfeld ,2014*).

ومن الملاحظ أن الدور الذي يمارسه هؤلاء الوكلاء السيبرانيين يتسم بصبغة سياسية حيث تتوجه جل الهجمات السيبرانية لدعم الأنظمة الحاكمة الموالية لإيران، أو نشر الخطاطة الشيعية في بلدانهم، أو للتعبير عن ولائهم للثورة الإسلامية بإيران.

لقد تزايد حجم التهديدات والهجمات السيبرانية وتنوعت أهدافها بشكل ملحوظ خلال السنوات الثلاث الأخيرة (*Nakashima,2014*)، فبلغ عدد الأهداف التي هاجمتها مجاميع قراصنة المعلومات والفصائل والبؤر السيبرانية التي تعمل تحت راية النظام الإيراني (خلال عام 2014 فقط) أكثر من 1,600 هدف وحساب يعود الى شخصيات مرموقة تعمل في مؤسسات عسكرية، أو القطاع الدبلوماسي، وباحثين في مؤسسات علمية رصينة، ورجال أعمال، وأكاديميين، وناشطين في مجال حقوق الإنسان، ورجال صحافة وإعلام، وآخرين ممن ينتمون الى جنسيات متنوعة، ويتوزعون على رقعة جغرافية واسعة بقصد التلصص على بياناتهم الشخصية، أو محتوى التواصل السيبراني داخل حدود مؤسساتهم الحيوية، وغيرها من المعلومات التي تدعم قدرات أجهزة الأمن والمخابرات الإيرانية (*Constantin,2015*).

بصورة عامة ينشط الجيش الإلكتروني السوري في مهاجمة أهداف حيوية تقع في قائمة خصوم بلاده، وتلتحق بقائمة خصوم إيران. ومن هذه الهجمات قيام فصائل هذا الجيش السيبراني بشن سلسلة من الهجمات وعمليات الاختراق التي طالت مجموعة من الحسابات التي تعود الى موقع *Microsoft's Xbox* وموقع الشبكة الإخبارية الشهيرة *CNN* مما أثر بشكل ملموس على حضورهما في الفضاء السيبراني العولمي (*IICT,2014*). كما استمرت فصائل هذا الجيش بدعم الفصائل السيبرانية الإيرانية من خلال اكتساح مواقع أخبارية غربية عن طريق اختراق حضورهم السيبراني وخدماتهم البريدية في كثير من الدول، شملت: إسرائيل، وتركيا، وقطر ودول في مجلس التعاون الخليجي (*IICT,2014*).

كذلك اتسمت هجمات الجيش السوري الإلكتروني باستهدافها لبوابات الأخبار والإعلام الغربي التي تناهض النظام السوري فتخترق حساباتهم على مواقع التواصل الاجتماعي (*Twitter&Facebook*) مع إيداع رسائل وتهديدات في هذه الحسابات. وكان على قائمة الجهات التي طالتها هذه الهجمات كل من: *The Financial Times,The Telegraph, the BBC, the AFP, The Washington Post, The Onion, NPR, The Guardian* بالإضافة الى قناة الجزيرة القطرية وقنوات خليجية تجهر بمناوئتها للنظام السوري والإيراني على حد سواء (*IICT,2013*).

بالمقابل تعد الهجمة التي مارستها فصائل هذا الجيش، (ضد حساب وكالة أخبار أسيوشيتد بريس على منصة التغريد السيبراني *Twitter*، في شهر أبريل من عام 2013) من أكثر الهجمات تأثيراً على المؤسسات الإخبارية الغربية، حيث نجحت الهجمة بإقحام مجموعة من الأخبار المزيفة حول حصول انفجارين في مقر الرئيس الأمريكي، باراك أوباما، في البيت الأبيض، والتي نشب عنها حصول خلل في أسواق رأس المال والبورصة الأمريكية، كلفت الولايات المتحدة الأمريكية خسائر ناهزت بضعة مليارات من الدولارات خلال مدة قصيرة جداً، ولحين تكذيب الخبر (*IICT,2013*).

كما وقامت إحدى المجاميع الملتحقة بالجيش الإلكتروني السوري بمهاجمة مضيفات خدمة البريد الإلكتروني التي تعود الى مؤسسات حكومية منتشرة في أكثر من بلد مناهض لسياسة النظام الإيراني، في محاولة لاختراق صناديق البريد الإلكتروني وتسريب معلومات مهمة ونشر حسابات البريد الإلكتروني وكلمات العبور لشخصيات سياسية مهمة.

وقد نجحت هذه الهجمات في اختراق البريد الإلكتروني لرئيس وزراء تركيا، ومكاتب حكومية في دولة قطر، وأخرى بوزارة الدفاع السعودية، وجامعة الدول العربية، ومواقع أخرى (*IICT,2013*).

أما كتائب عز الدين قسام التي تستوطن فضاء غزة السيبراني، فقد أعلنت في بداية عام 2012 عن قيامها بسلسلة هجمات على مؤسسات مالية أمريكية شملت مصرف أميركا، وسوق نيويورك للأوراق المالية في سبتمبر عام 2012 للتعبير عن حملة التشويه التي مورست ضد شخصية الرسول الكريم (ص) (*Siboni&Kronenfeld ,2014*).

كما قامت خلال الأمد الممتد بين سبتمبر 2012 ويناير 2013 بسلسلة هجمات رفض الخدمة (*DDoS*) ضد أهداف منتخبة في مؤسسات مالية أمريكية، منها: *Bank of America Corp, CitiGroup, JPMorgan, Chase and Wells Fargo* أحدثت فيها تأثيرات ضارة (*OB,2013*).

أما الفصائل السيبرانية لحزب الله اللبناني فتعبّر عن ولائها للنظام الإيراني من خلال الهجمات التي تقوم بها ضد المواقع والمصالح الصهيونية الاقتصادية المنتشرة في فضاء الإنترنيت.

رغم أن جيش فضاء اليمن السيبراني لم يعلن انتماؤه الى مجاميع قراصنة المعلومات الإيرانيين، إلا أن النشاطات السيبرانية التي يمارسها تصبّ في مصلحة النظام الإيراني لتوجيه دفتها ضد أهداف ومصالح تعود الى المملكة العربية السعودية، ودول خليجية قد التحقت بفريق التحالف العربي الذي يقاتل مع الشرعية في اليمن. بالمقابل نجح فريق الاستخبارات الأمريكي *Crowd Strike* في الكشف عن علاقة وثيقة بين هذه الفصائل السيبرانية ومجاميع قراصنة معلومات مثل: *EMAD* و*Parastoo* (*Crowdstrike,2015*).

كانت الهجمة الأولى لفصائل هذا الجيش في 13 أبريل من عام 2015 حيث اكتسح أفراد إحدى فصائله موقع جريدة الحياة التي أظهرت تعاطفاً مع التحالف العربي ووجهت أصابع الاتهام نحو الحوثيين وحليفتهم إيران، ولم يمر سوى بضعة أسابيع حتى شنّت هذه الفصائل هجمة أخرى اخترقت فيها شبكة موقع وزارة الخارجية السعودية في شهر مايو من العام ذاته (*Bicchirea,2015*) وباشر بالدخول الى قواعد البيانات حيث نجح بنشر الكثير من الوثائق السرية التي تخص نشاطات هذه الوزارة (*Crowdstrike,2015*).

كذلك عثر المتخصصون على أكثر من بصمة تؤشر الى مشاركة فصائل هذا الجيش ضمن تشكيلات جيش فضاء إيران السيبراني في الهجمة الشرسة التي طالت شركة أرامكو السعودية، وتسببت في إتلاف محتويات أكثر من 30 ألف حاسوب تعود الى موظفي هذه الشركة النفطية العملاقة (*Bicchirea,2015*).

ورغم صعوبة مسألة تحديد هوية الجهة التي تمارس التهديدات أو الهجمات السيبرانية بصورة قاطعة في بيئة فضاء الفيض السيبراني، وذلك لما تتسم به هذه البيئة من سمة بنيوية معقدة، مع تشابك خيوط مورد الممارسة، وتعدد مساراتها بين مجموعة من المضيفات السيبرانية التي قد تتوزع على مساحة جغرافية واسعة (*Siboni&Kronenfeld ,2014*) فقد نجحت مراكز البحوث (التي تعنى بدراسة البيئة الحاضنة للهجمات في البحث والتحري عن مصادر هجمات الوكلاء والبؤر السيبرانية الموالية لإيران) بتتبع آثار هؤلاء الوكلاء، فأعلنت مجموعة *HP Security* في تقريرها الصادر في شهر شباط من عام 2014 عن نجاحها في تحديد اهم مجاميع القرصنة الموالية للنظام الإيراني، من خلال المسح السيبراني الذي مارسته كوادرها أثناء تتبع موارد الهجمات، ومسارات أهدافها، وطبيعة تأثيراتها على الكيانات السيبرانية.

وقد عثرت المجموعة على قواسم مشتركة بين هذه المجاميع تؤكد هذا الانتماء والولاء الذي ترتبط به مع النظام الإيراني، أهمها :(*HP,2014*):

- ✓ أن اللغة الإيرانية كانت اللغة الأم التي استخدموها في تواصلهم السيبراني قبيل شن الهجمات، وأثنائها، وبعد استكمال سيناريو هذه الهجمات.
- ✓ ظهور بصمة تأثير خطاطة ثقافة الإسلامية في الخطاب الذي تحاول إلصاقه بالأهداف المنتخبة، ونشوبها كرد فعل مباشر على التجاذب والتدافع بين إيران وخصومها.
- ✓ يتعاملون مع العالم الغربي، وإسرائيل بوصفها كيانات معادية يحرصون على مجالدتها رقمياً.
- ✓ يوظفون مزيجاً من الأساليب التقنية، وأخرى غير تقنية في انتخاب أهدافهم السيبرانية.
- ✓ يحاولون الإعلان عن هجماتهم السيبرانية من خلال فضاء شبكات التواصل الاجتماعي، مع الحرص على إدراجها ضمن الأهداف التي يعلن عنها موقع أخبار القرصنة الشهير *Zone-H.*
- ✓ وجود صلات حميمة تجمع فيما بينهم، مع امتلاكهم لثقافة قرصنة معلوماتية متقدمة، مع حضور لقواسم مشتركة أسهمت الى حد كبير في ضمان تنسيق عال في أدائهم نشب عنه نجاح هذه الهجمات في تحقيق أهدافها بالفضاء الافتراضي.

5 . 3 . 5 . التحولات النوعية في التهديدات والهجمات السيبرانية الإيرانية:

لم يتوقف طموح النظام الإيراني عند عتبة التحول من النزعة الدفاعية باتجاه النزعة الهجومية (في فضاء المنازعة السيبرانية) بل توسعت دائرة دائرته باتجاه شنّ هجمات نوعية باتت تؤرق خصومها نتيجة لعمق تأثيراته، والتعقيد الذي تتسم به آلياتها، وخطورة الأهداف التي نجحت باختراقها.

لقد نجحت الفصائل السيبرانية الإيرانية، وعلى رأسها جيش فضاء إيران السيبراني، ومجاميع القرصنة المتحالفة معها مثل: Ashiyane و Ajax Team و Shabgard وبالتنسيق مع الفصائل السيبرانية الملتحقة بمنظمة الباسيج، والوكلاء السيبرانيين الذين يقيمون خارج حدود فضاء إيران السيبراني، في تحقيق طفرة نوعية، على صعيد السطوة السيبرانية، خلال السنوات التي تلت هجمة الفايروس Stuxnet والأجيال التي استنسلت من معماريته البرمجية فأضحت تتربع على إحدى المرتبتين الرابعة أو الخامسة على صعيد أقوى الجيوش السيبرانية في فضاء الفيض السيبراني.

لقد خطط الحرس الثوري الإيراني، الراعي الأكبر للغزوات السيبرانية الإيرانية، لهجمات اتسمت بتنسيق عال بين جميع الفصائل السيبرانية الإيرانية، ووكلائها السيبرانيين من داخل إيران وخارجها، وباستخدام تقنيات غير مسبوقة، منحتها الفرصة لاكتساح عدد كبير من الأهداف الاستراتيجية، وبعمق استراتيجي ملحوظ، وعلى رقعة جغرافية واسعة شملت بلداناً تستوطن أكثر من إقليم جغرافي، وقارة. وأثبتت قدرتها على شن هجمات كاسحة على أكثر من هدف، في أكثر من بلد، وخلال بعد زمني طويل المدى لحين كشف آثار هذه الهجمات.

وسنحاول تحليل ثلاث نماذج لهجمات انتخبناها من بين عدد لا بأس بها من الهجمات، ووقع اختيارنا عليها لكونها تمثّل قفزة نوعية على صعيد الهجمات السيبرانية ـ العولمية خلال السنوات الخمس الأخيرة الماضية.

الأنموذج الأول: عملية زهرة الزعفران Operation Saffron Rose:

عكفت شركة Fire Eye الأمريكية المتخصصة بمتابعة الهجمات السيبرانية في الفضاء السيبراني على تحليل تفاصيل الهجمة التي قامت بها مجموعة قراصنة المعلومات[228] Ajax Security Team الإيرانية والتي أطلق عليها اسم "عملية الزعفران Saffron Rose" (Villeneuve, et.,al.,2013).

عدّ الخبراء عملية زهرة الزعفران قفزة نوعية على صعيد عمليات التجسّس السيبراني، حيث وظفت مجموعة Ajax Security Team[229] تقنيات ذكية تستبطن سلوكها الجرمي وراء ستار خدمات دعم العاملين في مؤسسات البحث والتطوير في قطاعات الدفاع وقطاعات أكاديمية أخرى، وتوفير تسهيلات للمشاركة في المؤتمرات واللقاءات العلمية (Info,2013).

وقد سخّرت المجموعة لعمليتها برنامجاً خبيثاً للتلصص وسرقة البيانات Stealth Malware أعدّت معماريته البرمجية في مختبراتها في إيران. ويقوم البرنامج الخبيث بسرقة البيانات المستودعة في نظام إدارة المعلومات الذي استهدفته الهجمة، ويعمد الى تدوين جميع البيانات التي تخص: اسم الجهة المضيفة، وعنونتها على الإنترنيت، اسم المستخدم، البوابات السيبرانية المفتوحة، التطبيقات الموجودة في حاسب الضحية السيبرانية، هوية العمليات الجارية، قائمة المفاتيح Key Logging، لقطات ملتقطة من شاشات المستخدمين، حسابات البريد والتواصل الإلكتروني، والحسابات والمفضلات الموجودة على المستعرضات Browsers، وتفاصيل أخرى ذات صلة بأدق تفاصيل خصوصية المستخدمين (Scharr,2014).

وظفت المجموعة برنامجها الخبيث لشنّ أكثر من هجمة تجسس رقمي ضد شركات تعمل بقطاع الصناعة العسكرية بالولايات المتحدة الأمريكية، كما لم تسلم من آفتها حسابات شخصيات من المعارضة الإيرانية، ممن يستخدمون برامج اختراق جدران الحظر السيبراني[230](*Sandoval,2014*).

كذلك شملت الهجمة قيام المجموعة بالترويج لمؤتمرات ولقاءات دولية وهمية بقصد جذب العاملين في مجال البحث العلمي والتقني في أكثر من قطاع بالولايات المتحدة لاستدراجهم من خلال المواقع الوهمية للمؤتمرات حيث تمارس عملية الدخول الى حواسبهم الشخصية، والمكتبية، لسرقة كم كبير من البيانات الشخصية (*Jackson,2014*).

المثال الثاني: عملية الساطور *Operation Cleaver*:

شدّت تفاصيل عملية الساطور *Cleaver* اهتماماً عولمياً على صعيد الاختراق والمراقبة السيبرانية، والتي باشر أنشطتها التخريبية بواسطة فريق تألف من مجاميع مقيمة في طهران، وأخرى تقيم في هولندا، وكندا، وبريطانيا، وبتوظيف تقنيات بالغة التعقيد، مع تحقيق تأثير امتد على رقعة جغرافية واسعة، أسهم في بلوغ المجاميع المهاجمة أهدافاً بالغة الأهمية خلال بعد زمني متطاول.

---

[228] . يتألف قوام هذه المجموعة من مجاميع قراصنة معلومات إيرانيين، يمارسون نشاطاتهم من داخل حدود البلاد، مثل: مجموعة *Ashiyane*، ومجموعة *Shabgard*، وقراصنة آخرين عملوا سوية منذ عام 2010 تحت هذا الاسم لتنفيذ سلسلة هجمات على مواقع ويب لخصوم النظام الإيراني في الداخل والخارج، على حد سواء.

[229] . صنفت مجموعة FireEye مجموعة Ajax Security Team ضمن مجاميع التهديدات المتقدمة . المستمرة Advanced Persistent Threat (APT) (Info,2013).

[230] . مثل البرنامج Proxifier والبرنامج الشهير Psiphon واللذين يستخدمهما الإيرانيون بكثرة لتجاوز عقبة الحظر.

شملت أهداف هذه الغزوة السيبرانية موارد البنية التحتية لمجموعة واسعة من المؤسسات العولمية المهمة، والتي توزعت على قطاعات: شركات عسكرية، وشركات للنفط والغاز، وشركات خطوط جوية، وشركات منتجة لمصادر الطاقة، وشركات خدمية، ومؤسسات صحية، وشركات اتصالات، وشركات تقنية، ومؤسسات تعليمية، ومراكز تقنية فضائية، وقواعد للصناعة العسكرية، وشركات تعنى بالصناعات الكيمياوية، بالإضافة الى ثلة من المؤسسات الحكومية (*Siboni,et.,al.,2015*).

أما امتدادات الهجمة فقد انبسطت على رقعة جغرافية شملت: كندا، والصين، وبريطانيا، وفرنسا، وألمانيا، والهند، وإسرائيل، والكويت، والمكسيك، والباكستان، وقطر، والسعودية، وكوريا الجنوبية، وتركيا، والإمارات، والولايات المتحدة الأمريكية ـ أنظر الجدول (6- 3) للوقوف على هوية الشركات التي استهدفت في كل بلد من هذه البلدان (*Siboni,et.,al.,2015*).

الجدول (6- 3) ـ هوية الأهداف التي طالتها الهجمة في البلدان المستهدفة.

البلد	القطاعات المستهدفة
إسرائيل.	مؤسسات فضائية، مؤسسات تعليمية.
ألمانيا.	شركات اتصالات.
الإمارات.	مؤسسات حكومية، خطوط جوية.
الباكستان.	مطارات، مؤسسات صحية، مؤسسات تقنية، خطوط جوية.
بريطانيا.	مؤسسات تعليمية.
تركيا.	شركات نفط وغاز.
السعودية.	شركات نفط وغاز، مطارات.
الصين.	مؤسسات فضائية.
فرنسا.	شركات نفط وغاز.
قطر.	شركات نفط وغاز، مؤسسات حكومية، خطوط جوية.
كندا.	شركات طاقة وخدمات، شركات نفط وغاز، مؤسسات صحية.
كوريا الجنوبية.	مطارات، خطوط جوية، مؤسسات تعليمية، تقنية، صناعات ثقيلة.
الكويت.	شركات نفط وغاز، شركات اتصالات.
المكسيك.	شركات نفط وغاز.
الهند.	مؤسسات تعليمية.
الولايات المتحدة.	شركات خطوط جوية، مؤسسات تعليمية، شركات كيمياوية، شركات نقل، شركات طاقة وخدمات، مؤسسات حكومية وعسكرية، قواعد صناعات عسكرية.

المصدر: *Siboni,et.,al.,2015*.

وقد تباينت مستويات عمق المصاولة السيبرانية في كل مؤسسة أو شركة من الشركات التي نالتها الهجمة، كما اختلف تأثيرها باختلاف بلدان المعترك السيبراني[231]. فقد تدرجت آثارها بين إحداث خلل جزئي أو كلي في مضيفات ويب نظام ويندوز ونظام لينكس، أو اختراق البنية التحتية لشبكات المعلومات بكامل المعدات التي تقيم في نسيجها الشبكاتي، أو الوصول الى موارد المعلومات وقواعدها وتسريب بيانات مهمة يمكن استثمارها في هجمات مستقبلية.

ويمكن عرض أهم ما توصل إليه خبراء أمن المعلومات في شركة *Cylance* الأمريكية التي تتبعت آثار الهجمات في الدول التي كانت فريسة سائغة لهذه الهجمات ضمن المخطط المدرج في الشكل (6- 2).

إثبات أن إيران وراء هذه الهجمات

- إيراد أسماء إيرانية لقراصنة المعلومات الملتحقين بفصائل الغزوة السيبرانية ضمن معمارية الهجمات.
- جل أسماء النطاقات التي انطلقت من خلالها الهجمات تقع ضمن نظام أسماء النطاق في إيران.
- البنية التحتية التي وظفتها قراصنة المعلومات لشنّ هجماتها تعود الى مجموعة *Tarh Adinshan* الايرانية.
- استضيفت الهجمات في مضيفات تعود الى شركة *Netafraz.com* التي تقيم في مدينة أصفهان الايرانية.

التطور الحاصل في مهارات القرصنة الإيرانية

- توظيف تقنيات غير متطورة استخدمها قراصنة معلومات صينيون وآخرون في روسيا الاتحادية.
- تطوير أدوات القرصنة الشائعة وتسخيرها لتلبية احتياجات الهجمة ولضمان تحقيق غاياتها.
- القدرة على إنتاج أدوات قرصنة قادرة على تحقيق غايات محددة وبكلف زهيدة.
- حصول طفرة نوعية في التقنيات المستخدمة بهجمات القرصنة استرشدت بالمنطق المعقد والمعمارية غير المسبوقة التي اتسمت بها بنية البرمجيات الخبيثة التي استهدفت بواسطتها منشآت حيوية إيرانية.

الشكل (6- 2) ـ أهم ما توصل إليه الخبراء بصدد هجمة الساطور السيبرانية[232].

أشارت البيانات الأولية للبصمات السيبرانية (ذات الصلة بهذه الهجمة) أن بداياتها كانت عام 2013، وأنها استمرت لحين العثور على أثرها في إحدى الأهداف، وتوقع الخبراء أن فرضية عدم الكشف عنها تؤكد أن آثارها كانت ستتطور بشكل كبير، وأنها لو تواصلت كانت ستحدث تأثيرات تخريبية وخيمة على مستوى الأمن السيبراني العولمي (*INSS,2014*).

ولم تتوقف الفصائل السيبرانية الإيرانية التي تعمل ضمن تنظيمات جيش فضاء إيران السيبراني، أو تلك التي تدين بالولاء لمؤسسات عسكرية، أو أمنية، أو مجاميع مستقلة عند هاتين الهجمتين التي عدّها خبراء أمن المعلومات من الهجمات النوعية، بل استمرت في شن هجمات مماثلة، نذكر منها قيام مجموعة قراصنة المعلومات *Parastoo* بهجمة

[231] . بلغ عدد الأهداف التي بلغتها هذه الهجمة أكثر من خمسين هدف حيوي.

[232] . أعد هذا الشكل من البيانات التي وردت في تقرير شركة Cylance المفصل عن هذه الهجمة (*Siboni,et.,al.,2015*).

في 25 نوفمبر من عام 2012 نجحوا فيها باختراق حواسب الهيئة الدولية للطاقة الذرية *International Atomic Energy Agency (IAEA)*، على التوازي مع حواسب وزارة الطاقة الأمريكية *United States Department of Energy*، للتعبير عن سخطهم عن الضغوط المستمرة التي تمارس على البرنامج النووي الإيراني (*IDC,2014*).

كذلك هناك الهجمة الشرسة التي قامت بها مجموعة من الإيرانيين ونجاحها في اختراق منظومة تشغيل سد *Bowman Avenue Dam* في مدينة نيويورك، في الربع الأخير من عام 2013، قلقاً متزايداً لدى إدارة البيت الأبيض، وحرص كل من مكتب التحقيقات الفيدرالي *FBI*، وقسم الأمن الوطني *Department of Homeland Security (DHS)* على عدم الإفصاح عن هذه الهجمة الخطيرة في وسائل الاعلام الأمريكية (*Dodrill,2015*)، بيد أن أحد مراسلي صحيفة *The Washington Post* قد فجّر القنبلة الإعلامية وأعلن عن تفاصيل الهجمة بعد أن بقيت طيّ الكتمان لمدة سنتين تقريباً (*Vijayan,2015*).

لقد أقضّت نتائج هذه العملية مضاجع الإدارة الأمريكية، وعمّقت قلقها حول تراجع حصانة المنظومات المتقادمة التي تستخدم في إدارة نظم المعلومات لأكثر من 57 ألف منظومة تحكّم محوسب في ميدان الصناعات الأمريكية، بالإضافة الى شبكات توزيع الطاقة في عموم الولايات المتحدة، والتي باتت تمثل أهدافاً سهلة لمثل هذه الهجمات التي توظف خوارزميات برمجية معقدة، قادرة على ممارسة عملية الاختراق بسهولة ويسر (*Dodrill,2015*).

ويضاف إليها عثور مجموعة من الباحثين في شؤون أمن المعلومات بالولايات المتحدة في عام 2014 على أكثر من بصمة رقمية تؤكد قيام قراصنة معلومات إيرانيين بسلسلة هجمات على مواطنين أمريكان ينحدرون من أصول إيرانية، ممن يعملون بعقود ومقاولات مع وزارة الدفاع الأمريكية، والمملكة المتحدة، وإسرائيل، بالإضافة الى مجموعة من صنّاع القرار، وشخصيات عسكرية مرموقة بوزارة الدفاع الأمريكية للتجسس على مراسلاتهم وأنشطتهم المختلفة. وقد تزايد عديد هذه الهجمات أثناء المباحثات الإيرانية مع الدول الكبرى حول ملفها النووي، بحيث تجاوزت 1,500 هجمة خلال مدة قصيرة كرد فعل مباشر ضد النهج الذي تنتهجه الولايات المتحدة وحليفاتها ضد المشروع النووي الإيراني (*Snapshots,2015*).

وعلى صعيد آخر، عثر أحد الباحثين الأمريكيين في جامعة كاليفورنيا على بيانات أرشدته الى قيام قراصنة معلومات إيرانيين[233] باختراق قواعد بيانات تعود الى منظومة إدارة نقل الطاقة الكهربائية. بدأت محاولة الاختراق في شهر أغسطس عام 2013 ويبدو أنها لا زالت مستمرة في جمع بيانات مهمة من أكثر من مورد ذو صلة بمنظومات نقل الطاقة بالولايات المتحدة[234]. و من جانبها، ذهبت شركة *FireEye Inc.* إحدى كبريات الشركات التي تعنى بملف أمن المعلومات في وادي السيليكون، بالولايات المتحدة، الى إدراج مجموعة قراصنة المعلومات الإيرانيين *Ajax Security Team* على رأس قائمة قراصنة المعلومات الإيرانيين التي نجحت باستخدام برمجياتها الخاصة لطمر الشيفرات البرمجية الخبيثة التي مارست دور التلصص السيبراني واستراق البيانات من المستودعات السيبرانية لمجموعة من الشركات المتخصصة بالصناعات العسكرية في الولايات المتحدة (*Finkle,2014*).

233 . استطاع الباحث تحديد هوية القراصنة من خلال الملاحظات المودعة في الإيعازات البرمجية، والتي دوّنت باللغة الفارسية.

234 . نجح قراصنة المعلومات الإيرانيين في الحصول على التصاميم الهندسية ورسومياتها التفصيلية لأكثر من شبكة نقل، ومحطات التوليد المرتبطة بها، والتي يمتد توطنها الجغرافي بين نيويورك وكاليفورنيا.

ورغم أن الخبير الإسرائيلي جابوني سيبوني قد قلل من احتمالية نجاح عمليات استهداف البنى التحتية للطاقة الكهربائية، ومنظومات تغذية مياه الشرب، وإدارة المطارات ووسائل المواصلات، بسبب افتقار مثل هذه الهجمات الى قدرات غاشمة في مضمار اختراق نظم المعلومات وشبكات الاتصالات التي تهيمن على إدارتها نظم بالغة التعقيد، واستبعد حصول مثل هذه التهديدات في الوقت الراهن، إلا أنه عاد ورفع من مستوى الاحتمال عند مراجعته لملابسات الهجمات السيبرانية التي شنتها روسيا الاتحادية على أوكرانيا في 23 ديسمبر من عام 2015، حيث حصل توقف مفاجئ في شبكة التوليد الغربية للبلاد، بعد أن توقفت ثلاثة محطات لتوليد الطاقة الكهربائية، على التوازي مع حصول في 26 محطة توزيع للطاقة في ذلك القطاع نتيجة لحصول اختراق أمني في شبكة المعلومات الأوكرانية. وبصرف النظر عن وجهة أصابع الاتهام التي وجهتها الإدارة الحكومية الإيرانية نحو شركات أمنية روسية ملتحقة بالحكومة الروسية، فإن مثل هذا التهديد الذي فرض نفسه على أرض الواقع، ومن خلال ممارسة هجمات معلوماتية، عاد ليؤشر الى أن الاحتمال أصبح قائماً، وأن تأخر حضوره لدول أخرى ذو صلة بكفايتها الأمنية، وفق المعايير الراهنة، وأن أي خلل في الكفاية، أو ولادة ثغرة رقمية ـ أمنية غير منظورة سيجعل من أي دولة عرضة لمثل هذه التهديدات وآثارها الخطيرة (*Siboni&Magen,2016*).

ويؤكد تنامي المخاطر التي قد تنشب عن التطور النوعي في الهجمات الإيرانية، خلال السنوات 2012-2015 ما أفصحت به بعض الوثائق الاستخباراتية التي سرّبت على موقع ويكي ليكس عن تنامي القلق لدى وكالة الأمن القومي *NSA* بالولايات المتحدة الأمريكية من تهديد خطير لأمن فضاء الفيض السيبراني بالولايات المتحدة نتيجة لاكتشاف أداة رقمية إيرانية (سلاح رقمي خطير) تمتلك القدرة على اكتشاف الثغرات الأمنية المقيمة في شبكات المعلومات. لقد وصفت الوكالة هذا السلاح بالخطير، والذي ألجأها الى طلب الدعم من المملكة المتحدة للتعاون في احتواء التأثيرات المحتملة لهذا السلاح السيبراني ـ الخطير (*Brunner,2015*).



وصل و خاتمة

وصل وخاتمة

اشتهر الشعب الإيراني بشدّة شغفه وولعه العميق باستخدام الإنترنيت، والحضور في فضائها السيبراني المتخيّل، حتى عدّه البعض أنموذجاً حياً لشعب من الشعوب الافتراضية التي تحرص على إدامة الإقامة والحضور في فضاء الفيض السيبراني *Cyber Nation*. ولعل من أكثر المبررات قبولاً لهذا الشغف العميق هو قدرة هذا الفضاء على اصطناع مناخ بديل، متخيّل، يمارس دور البديل لفضاء الواقع الفيزيائي، الذي يحفل بعقبات وإشكاليات تعترض ممارساته اليومية نتيجة لما تلقاه من معارضة شديدة من مؤسسات النظام الإيراني السياسية والعقدية بدواع مخالفتها لخطاطة ثقافة الثورة الإسلامية الإيرانية (*Baker,2015*).

ولم يشكل هذا الحضور العميق، في بداياته، سوى قلقاً بسيطاً لدى المؤسسات الأمنية والعسكرية بداع التهديدات المحتملة لثقافة الثورة الإسلامية ومبادئها، والذي شاركتهم فيه الجهات الحوزوية بوصفها المسؤول المباشر عن حماية الخطاطة العقدية للإيرانيين. فمورست عمليات مراقبة المحتوى السيبراني، وحظر المواقع التي تعد مخالفة لمبادئ الثورة الإسلامية، إضافة الى تتبع ممارسات القرصنة السيبرانية التي مارسها قراصنة هواة، أو آخرين ينتمون الى المعارضة الإيرانية.

وكما أن حضور الإنسان في مجتمعات المعرفة المعاصرة، بدأ تدريجياً بالتحول نحو الحضور السيبراني، في فضاء متخيل تمارس فيه عمليات التواصل الاجتماعي عبر قنوات شبكات التواصل السيبراني، بعيداً عن التواصل وجهاً لوجه، على أرض الواقع الصلبة، كذلك فإن ممارسة التهديدات وشن الهجمات على الخصوم لم تعد تفتقر الى منازلة تلزمنا بالانتقال نحو حياض الخصم متجشمين أنواع المكابدة في قطع المسافات، والتقلب بين البلدان، بعد أن برز فضاء الفيض السيبراني بوصفه فضاءً بديلاً، يمكن أن تمارس في مجاله السيبراني المتخيّل، شتى أنواع الممارسات التي يمكن أن تحمل في قنواتها السيبرانية مختلف أشكال التهديدات، وتشنّ من خلالها أشد الهجمات فتكاً في الكيانات السيبرانية المناظرة لوجودنا في فضاء الواقع.

لم يعد من الضروري تجحفل الفصائل المتنازعة في ساحة الوغى، بعد أن تحوّلت ساحة المجالدة الى طرفيات ترتبط بالبوابات السيبرانية لفضاء الفيض السيبراني، ويعكف على استخدامها مجموعة من الفصائل والميلشيات السيبرانية، التي تدين بالولاء لهذا النظام أو ذاك، فتكتسح البنى التحتية للمعلومات والاتصالات، وتورث مختلف أشكال الكيانات السيبرانية التي تقيم في الفضاء المتخيل، خللاً في الأداء، أو تشويشاً في المشهد، أو يتفاقم تأثيرها بحيث تفلح بالقفز خارج حدود الفضاء المتخيل باتجاه منظومات التحكم في تسيير دفة منظومات إنتاج الطاقة، وإدارة النقل والمواصلات، أو المنظومات المتحكمة بتشغيل السدود المائية، بحيث يتسبب عنها كوارث تفوق تأثيراتها الهجمات التقليدية.

ولم تفلح سوى ثلاثة من الدول الكبار (هي الولايات المتحدة، وروسيا، والصين) في ترسيخ حضورها بفضاء المنازعة السيبراني، بعد أن رضيت بقية الدول في استخدام مجال الفضاء المتخيّل بعيداً عن فرض السطوة، أو ممارسة التنازع مع الغير، وسعت الى تشكيل كفاية أمنية مقبولة لحماية موجوداتها السيبرانية التي بدأت تستوطن في الفضاء السيبراني.

ولم تختلف إيران في توطيد حضورها عن بقية البلدان، وأكدت هذا الأمر نتائج الدراسة التي أجرتها مجموعة من الباحثين في عام 2005 (حول سمات البيئة الحاضنة لعلوم وتقنيات وممارسات أمن المعلومات في إيران) أن مسألة الأمن والردع السيبراني لم تقع (في بداية الألفية الجديدة) ضمن أولويات واهتمامات الحكومة الإيرانية، فلم تضعها ضمن خططها المستقبلية

(*Patterson&Smith,2005*)، كما أنها لم تبدي اهتماماً ملموساً بتطوير قدراتها لممارسة هجمات معلوماتية على مواقع ويب خصومها، أو ممارسة أنشطة لدرء الهجمات التي مارسها أعداؤها على مواقعها، ولكن انحصر اهتمامها بتطوير بنيتها التحتية للمعلومات والاتصالات، مع تعميق المعرفة بتفاصيل ملف أمن المعلومات وممارساته لدى كوادرها الوطنية، مع تنشيط قطاع إنتاج وتجارة أدوات المعلومات والاتصالات في السوق المحلية (*Arquilla&Borer,2007*).

وقد أثمرت الجهود الحثيثة التي بذلها النظام الإيراني لتطوير وتوسيع نطاق البنية المؤسسية التي تخطط، وتشرف، وتمارس الأنشطة ذات الصلة بعمليات الدفاع والردع السيبراني بعموم إيران. وقد أسس المجلس الأعلى لالفضاء السيبراني بوصفه الجهة العليا التي تستوطن قمة الهرم المؤسسي، والتحقت به قيادات النظام بدءاً برئيس الجمهورية، ونخبة من وزراء الجهات المعنية بفضاء الفيض السيبراني، والبنية التحتية للاتصالات، والأمن الوطني، والمؤسسة العسكرية، إضافة الى نخبة من الخبراء والقيادات التي ينتخبها المرشد الأعلى للثورة بصورة مباشرة. وتسري جميع قرارات المجلس الأعلى لالفضاء السيبراني نحو المركز الوطني لالفضاء السيبراني *National Cyber Center (NCC)* الذي يعد حلقة الوصل بين المجلس الأعلى وبقية البنى المؤسسية التي أنيطت بها مسؤولية أمن الفضاء السيبراني وإدارة أنشط الدفاع والردع السيبراني. وتتألف البنية المؤسسية هذه من قسمين، قسم تنهض به المؤسسات الملتحقة في سلك الحكومة، وآخر يعمل خارج حدودها. أنظر الجدول (1).

الجدول (1). تشريح البنية المؤسسية للدفاع والردع السيبراني الإيراني.

القسم الأول		القسم الثاني	
الجهة	الجهة الملتحقة بها	الجهة	الجهة الملتحقة بها
قيادة عمليات دفاع الفضاء السيبراني.	منظمة الدفاع المدني / القطاع العسكري.	مؤسسة الحرس الثوري الإيراني.	وحدة الحروب السيبرانية والالكترونية.
هيئة تمييز المحتوى الجنائي لمواقع الويب.	المجلس الأعلى للثورة الثقافية.		مجاميع قراصنة المعلومات المستقلين.
شرطة فضاء إيران السيبراني *FATA*.	مؤسسة الشرطة الإيرانية.	منظمة الباسيج.	مجلس الباسيج لالفضاء السيبراني.
مركز مهر لأمن المعلومات.	وزارة تقنية المعلومات والاتصالات.		

بصورة عامة تنصبغ الوحدات التنظيمية الموجودة في القسم الأول بصبغة دفاعية صرفة، حيث قد كلفت جميعها بمهمة الدفاع عن الفضاء السيبراني الإيراني من الهجمات التي تحاول النيل منه، سواء كانت هجمات تحاول إحداث تأثيرات ضارة في البرامج والمشاريع الاستراتيجية، أو الكيانات السيبرانية الإيرانية (تقوم بهذه المهمة كل من قيادة عمليات دفاع الفضاء السيبراني وبالتنسيق مع مركز مهر لأمن المعلومات)، أو كانت عبارة عن هجمات لينة تحاول إحداث خلل في منظومة ثقافة الثورة الإسلامية ومنجزاتها على أرض

الواقع(تقوم شرطة فضاء إيران السيبراني بحماية الفضاء الوطني من هجمات الجهات المعارضة لخطاطة النظام، بينما تقوم هيئة تمييز المحتوى الجنائي بالتنسيق مع الجهات المعنية في حظر المواقع أو المحتوى المناهض لثقافة الثورة الإسلامية).

على الطرف المقابل، نلاحظ أن الهيكلة المؤسسية للقسم الثاني قد انصبغت بصبغة الردع السيبراني، حيث تشترك مؤسسة الحرس الثوري الإيراني، مع منظمة الباسيج في قيادة مجاميع من الميليشيات والفصائل السيبرانية التي تنتمي إليها، بصورة مباشرة، أو تدين بالولاء والانتماء التام لبرامجهما، مثل مجاميع قراصنة المعلومات الإيرانية الشهيرة، بالإضافة الى متطوعين من مؤسسات أكاديمية وبحثية، وآخرين ممن يحسنون مهارات القرصنة من عامة الشعب الإيراني، في تكوين كيان افتراضي أطلق عليه اسم جيش فضاء إيران السيبراني *ICA* والذي أضحى يمثل الذراع السيبرانية الغاشمة للنظام الإيراني التي توجه ضربات رقمية موجعة للمعارضة الإيرانية، والى مناهضي النظام في منطقة الشرق الأوسط، أو الدول الكبرى التي تقف عائقاً أمام برنامجه النووي وبرامج التسليح البالستي التي تحرص مؤسساته على تطويرها.

من جهة أخرى فقد أسهمت سمة تعدد الطبقات التي تميزت بها الوحدات التنظيمية المكلفة بمهام الدفاع والردع السيبراني الإيراني، مع وجود قيادة موحدة، هي المجلس الأعلى لالفضاء السيبراني الإيراني في إحكام سيطرة النظام الإيراني على كل صغيرة وكبيرة تخص عمليات الدفاع عن الحياض السيبرانية الإيرانية، مع توحيد صفوف الجهات مجتمعة عند ممارسة أي عملية ردع رقمي ضد أهداف خصوم إيران، أو مناوئيها.

ويمكن أن نتلمس ولادة القدرات السيبرانية لدى الموارد البشرية الإيرانية في المؤسسات الأكاديمية، والعلمية التي ارتبطت مبكراً بفضاء الانترنيت، فأولت اهتماماً بتطوير مهاراتها للتعامل مع الفضاء الجديد بكفاءة.

وبدأت المؤسسات الأكاديمية بزج مناهج الحوسبة، وبمختلف مجالاتها، في مناهجها الدراسية، وحفلت مخابرها بتطبيقات ومراجعات حول التعامل مع الفضاء الجديد بأدواته السيبرانية، وتطبيقاته البرمجية.

من جانب آخر، بدأ المستخدم الإيراني بتطوير مهاراته الشخصية، وبناء قدراته على صعيد الاستخدام الأمثل للحاسب، والابحار في فضاء الانترنيت، واضطر نتيجة للقيود الصارمة التي فرضها النظام الإيراني على استخدامات فضاء الانترنيت الى تطوير مهاراته على صعيد القرصنة السيبرانية، وتجاوز الحواجز السيبرانية التي وظفها النظام لحجب التطبيقات، وحظر المواقع، فبدأت هذه المهارات تتطور، وتتصاعد مستوياتها على التوازي مع التصعيد الأمني الذي مورس على استخدامات فضاء الفيض السيبراني الذي انجذب اليه المستخدم الإيراني بقوة.

وتظهر عملية التنقير في حفريات الحضور السيبراني الإيراني، على صعيد القرصنة السيبرانية، أن إيران استطاعت أن تطوّر قدراتها السيبرانية من ممارسات بدائية لمستخدمين هواة وقراصنة مبتدئين، لم يفلحوا سوى باختراق بعض المواقع المحلية، غير الحصينة في بداية عام 2002، الى مارد رقمي رسّخ حضوره بعد عقد من الزمن، وباتت هجماته تهدد البنية التحتية لدول كبرى مثل الولايات المتحدة، وبريطانيا، وفرنسا، والصين، وأخرى عريقة بمهاراتها السيبرانية مثل الكيان الصهيوني.

لقد تبنى النظام الإيراني سياسة ذكية، توجهت نحو استدراج قراصنة المعلومات المحليين نحو إنشاء شركات أمنية محلية، ثم استطاعت إقناعهم باللّين، أو بالقوة، وأجبرتهم على الانصياع للعمل بمعية مؤسساتها العسكرية والأمنية[235]، وتبني خططاتها السياسية في التعامل مع مواقع خصومها بالولايات المتحدة، ودول أوربية تناصبها العداء، إضافة الى عدد من دول منطقة الشرق الأوسط، فتطورت قدراتها، وانبسط سلطانها وتعزّز على مساحة واسعة من القدرات البشرية التي تمتلكها نخبة إيرانية ماهرة في هذا المجال.

وبدأت مؤسسة الحرس الثوري تفكر جدياً في تشكيل فصائل تنهض بمهمة الدفاع عن الحياض السيبرانية للثورة الإيرانية، منذ بدايات عام 2005، بيد أن هذا المقترح لم ينل اهتماماً كافياً لحين ولادة الانتفاضة السيبرانية خلال الحملة الانتخابية لعام 2009، والتي شكلت بداية اليقظ لدى النظام الإيراني نحو إرساء أمن رقمي داخل حدود الفضاء السيبراني المحلي، فاستنهضت منظمة الدفع المدني، وشرطة فضاء إيران السيبراني للامساك بتلابيب الأمن السيبراني الوطني، وكف نشاطات المعارضة، التي حرصت على مناوئة النظام الإيراني.

وجاءت هجمة الفايروس الخبيث *Stuxnet* عام 2010 لتوقظ إيران من سباتها ولتجبرها على استنهاض جميع قدراتها لاحتواء آثار الهجمة الشرسة على مشروعها النووي، ومراجعة سياساتها بصدد ملف الأمن الوطني السيبراني، وإعداد العدة للدخول بقوة الى ساحة السجال السيبراني.

وقد تقاسمت مهمة السجال السيبراني مجموعة من المؤسسات الحكومية، ومتطوعين في منظمة الباسيج، ومجاميع من قراصنة المعلومات المحليين. فعلى صعيد المؤسسات الحكومية تنهض مؤسسة الحرس الثوري الإيراني بالجزء الأكبر من هذه المهمة، فتمارس دور العقل المسؤول عن إدارة المهام، والتخطيط المسبق، والإشراف المباشر على العمليات التي يقوم بها جيش إيران السيبراني بالإضافة الى بقية الكيانات التي تحتل أماكن مختلفة في البنية الهرمية لهذه التنظيمات، بينما تقوم منظمة الباسيج بتسخير فصائلها السيبرانية لدرء آثار الحروب الناعمة التي تحاول التسلل الى منظومة ثقافة الثورة الإسلامية، بينما تمارس شرطة فضاء إيران السيبراني مهمة تتبع المخالفات والتلصص على ممارسات المستخدمين التي تتعارض مع خطاطة النظام، أما هيئة تقدير المحتوى الجنائي لمواقع الإنترنيت فتنهض بمهمة مراجعة محتوى المواقع المقيمة في فضاء الإنترنيت وتحديد هوية المخالف منها ليتسنى للجهات المعنية بحظرها وكف عملية الوصول إليها.

لقد شهدت إيران نهضة كبيرة على صعيد بناء القدرات بعد عام 2010، حيث تكاتفت جهود جميع المؤسسات الأكاديمية، والبحثية، ومراكز التدريب في إعداد برامج تدريبية متقدمة لبناء القدرات الوطنية في مجالي الدفاع والردع السيبراني، والتحقت بهذا الركب مجاميع قرصنة المعلومات وأفصحت عن خبراتها العميقة في مجال القرصنة، بعد أن مارست مؤسسة الحرس الثوري الإيراني، ضغوطها على هذه المجاميع لتفصح عن خبراتها وترتقي بالمهارات الأكاديمية الى مستوى يتناسب مع التقدم الكبير الذي حققته على صعيد منتديات القرصنة السيبرانية . العولمية[236].

---

[235] . مع حلول عام 2010 أعلنت الوزارة الدفاع الإيرانية أن هناك أكثر من 1500 قرصان معلوماتي من إيران قد التحقوا ضمن فصائل مؤسسة الدفاع المدني الإيرانية لدرء المخاطر عن الحياض السيبرانية الوطنية.

[236] . عزت مراكز البحوث الغربية، التطور اللافت في قدرات الردع السيبراني الإيراني، الى نجاحها في لملمة جميع العناصر القوة التي تمتلكها على صعيد الموارد البشرية التي تمتلك خبرات عميقة في تقنية المعلومات والاتصالات وأمنها، والموارد التقنية وبراءات الاختراع التي نجحت مؤسساتها الأكاديمية ومراكزها البحثية في ابتكارها وتصنيعها، والخبرات الامينة والذراع

ولم تعد خصوم إيران قادرة على إنكار تطور القدرات لدى الموارد البشرية الإيرانية، فأقر خبراء أمن الفضاء السيبراني الإسرائيلي بالتطور اللافت لدى الموارد البشرية الإيرانية وآليات الهجمات التي استهدفت البنية التحتية للجيش الإسرائيلي بالإضافة الى مجموعة مهمة من المؤسسات المالية، أثناء اندلاع عملية حافة الوقاية *Protective Edge* ضد قطاع غزة عام 2013، وأنها باتت تمتلك سطوة رقمية منحتها القدرة على شن هجمات واسعة النطاق، وعلى أكثر من هدف وكيان رقمي حيوي، وباستخدام طيف واسع من تقنيات الاختراق السيبراني التي باتت تؤرق الفصائل السيبرانية التي تعمل تحت مظلة الجيش الصهيوني (*Siboni&Kronenfeld,2014*).

ورغم ادعاء الفصائل السيبرانية للجيش الصهيوني أنها قد نجحت باحتواء آثار هذه الهجمات بسرعة دون حدوث تأثيرات ضار، إلا أن الخبراء الصهاينة اعترفوا أن مصدر القلق من هذه السطوة المتنامية لن يزول في المستقبل القريب، لوجود أكثر من فرصة لشن غارات رقمية جديدة، واغتنام وجود ثغرة رقمية، قد تمنح للفصائل الإيرانية بالوصول الى هدف ثمين قد يكلف الكيان الصهيوني ثمناً غالياً (*Siboni&Kronenfeld,2014*).

ولم تعد إيران قادرة على التعامل مع التهديدات المستمرة، دون وجود استراتيجية واضحة المعالم تحدد كيفية التعامل معها على نطاق يتلاءم مع حجم هذه التهديدات، فولدت الاستراتيجية الدفاعية لالفضاء السيبراني الإيراني في مجال النزاع المستمر للنظام مع المعارضة في الداخل، وحرصه على درء الهجمات الناعمة واللينة التي مورست من خلال بث مادة المحتوى السيبراني الذي يناوئ الخطاطة السياسية والعقدية والثقافية للثورة الإسلامية.

ولم تكن ممارساتها، في البداية، ترقى الى مستوى الاستراتيجية وانحصرت في سياسة تبنتها المؤسسة الحوزوية التي نافحت عن الخطاطة العقدية والثقافية للنظام، بينما تكفلت مؤسسة الحرس الثوري الإيراني، ومنظمة الباسيج بتتبع آثار حضور المعارضة، والسعي الى اجهاض محاولات نشر خطابها المعارض في فضاء الانترنيت المحلي.

بيد أن وقائع فضاء النزاع السيبراني وتزايد حجم الهجمات التي باتت تنهمر على الكيانات السيبرانية الإيرانية منذ عام 2009، والتي بدأت تتطور باتجاه هجمات ذات بعد استراتيجي، بحيث نجحت في بلوغ الطبقات العميقة من منظومة أمن المشروع النووي الإيراني، والتسلل الى مؤسسات إيرانية بالغة الأهمية باتت تؤرق النظام الإيراني، وأجبرته على إعادة التفكير بانتخاب عناصر استراتيجيته الدفاعية، وتشكيل هذه العناصر بخطاطة جديدة تتناسب مع حجم التهديدات التي أضحت مؤثرة بشكل واضح.

من أجل هذا تبنى النظام الإيراني استراتيجية دفاعية جديدة، وضعت نصب عينيها مسألتين مهمتين (*Siboni&Kronenfeld,2014*):

العسكرية لمؤسسة الحرس الثوري الإيراني، والفصائل الملتحقة بها، بالإضافة الى حشد جميع الطاقات التي تمتلكها مجاميع قراصنة المعلومات الإيرانيين، وتحويلهم الى ميلشيات رقمية تعمل بمعية مؤسسة الحرس الثوري الإيراني، والتوجه نحو تشكيل بؤر رقمية خارج البلاد يقطنها وكلاء رقميون يدينون بالولاء للثورة الإسلامية، ويتفقون مع خطاطتها السياسية والعقدية، لإنتاج خليط متجانس، من المهارات والموارد التي تميز نسيجها بسمات مميزة، ودعم تفوقها على صعيد حروب فضاء الفيض السيبراني بشكل لافت (*Siboni&Kronenfeld,2014*).

(الأولى): تركيز الاهتمام بتطوير القدرات الدفاعية ـ السيبرانية للبلاد، على مستوى إعداد وتدريب الموارد البشرية الماهرة، وتطوير آلتها المادية (منتجات رقمية وبرمجيات متخصصة) بحيث تكون قادرة على صد الهجمات التي تمارسها المعارضة، وتلك التي تمارس من قبل الجهات التي تناوئ النظام وتحاول خلخلة فضائه السياسي، والتقني، والعقدي.

و**(الثانية):** التوجه نحو تطوير قدرات الردع السيبراني لمنح البلاد فرصة لمواجهة التفوق الكبير للعدو الأكبر (الولايات المتحدة الأمريكية) وترسيخ قدم النظام في فضاء النزاع السيبراني بحيث تسهم السطوة السيبرانية للنظام في التقليل من الهجمات التي تحاول النيل من البنى التحتية الوطنية، أو تلك التي تحاول خلخلة محيط الثورة الإسلامية بمجالاته السياسية والعقدية والثقافية.

وبدأت بوادر الاستراتيجية الجديدة بالنضوج خلال مدة زمنية قصيرة، نتيجة للآثار الوخيمة التي أصابت أجهزة الطرد المركزي الإيراني بعد تغلغل الفايروس الخبيث *Stuxnet*، ثم لم تلبث أن رسخت حضور حصانة رقمية رصينة، تتسم بتعدد مستوياتها، وتطور تقنياتها لضمان الدفاع عن البنى التحتية المهمة في إيران، مع حماية موارد البيانات الحساسة ضد الهجمات السيبرانية المحتملة من خارج البلاد. بالإضافة الى هذا يعد مشروع الانترنيت الوطنية *SHOMA* جزءاً لا يتجزأ من الاستراتيجية الدفاعية ـ السيبرانية لإيران، حيث سيسهم تشغيل هذا المشروع، الذي طال انتظاره نتيجة لكثرة تعثراته التقنية، في عزل فضاء إيران السيبراني عن الفضاء العولمي، وكف التدخلات والهجمات من الخارج، مع إحكام مراقبة أنشطة المعارضة وإحباط محاولاتها. كما سيسهم تشغيل هذه الشبكة بترسيخ حضور ما أطلق عليه "شبكة الانترنيت الحلال" التي ستحافظ على المحتوى السيبراني بعيداً عن كل ما يخالف الخطاطة العقدية للمؤسسة الحوزوية بإيران (*Siboni&Kronenfeld,2014*).

وقد قامت مؤسسة الحرس الثوري الإيراني، وبالتنسيق مع منظمة الباسيج، ومركز مهر لأمن المعلومات، وجهات أخرى تقع على مسؤولياتها حماية الحياض السيبرانية للبلاد، بإجراء مناورات ميدانية لاختبار القدرات الدفاعية السيبرانية، وتقييم مستوى نجاعة الاستراتيجية الوطنية. وكانت المناورة الأولى في بداية عام 2013 حيث اختبرت مؤسسة الحرس الثوري الإيراني القدرات الدفاعية لنظم المعلومات في مؤسسات النظام المختلفة، أما الثانية فأجريت في السنة ذاتها وبإشراف مباشر من قبل منظمة الدفاع المدني *PDO* والتي اختبرت خلالها حصانة الدفاع السيبراني للمنشآت النووية، ومترو طهران، وهيئة الإذاعة الإيرانية، والمصرف الإيراني المركزي، ومجهزي شبكة الاتصالات الخليوية[237] (*Siboni&Kronenfeld,2014*).

ولم تمر سوى بضعة حتى توجهت إيران نحو بناء قدرات الردع السيبراني بوصفها أداة ناجعة لتحقيق عدة غايات، (الأولى) وجدت إيران في حروب فضاء الفيض السيبراني مناخاً مناسباً لممارسة هجمات على أهداف خصومها الكبار من خلال تبني ممارسات الحروب غير المتساوقة *Asymmetrical Warfare* والتي لا تفتقر الى حجم كبير من الموارد في إحداث تأثيرات ضارة قد تنال البنى التحتية لتوليد الطاقة، والمؤسسات المالية، ومنظومات إدارة النقل لدى خصومها *(Siboni&Kronenfeld,2012)*، و(الثانية): درء المخاطر المتزايدة على البنية التحتية للبلاد نتيجة للضغوط التي يمكن لإيران أن تمارسها على الخصوم من خلال تصعيد

[237]. أظهر التقرير الذي أعدته منظمة الدفاع المدني بعيد إجراء هذه المناورة وجود ثغرات وفجوات رقمية يمكن لأعداء إيران استغلالها في تنفيذ هجمات على الفضاء الوطني، كذلك استصدر قرار بإنشاء مركز للدفاع السيبراني في مشروع نطنز النووي لعدم كفاية التشكيل القائم في توفير الحماية المطلوبة لهذا المشروع الاستراتيجي.

الهجمات المعاكسة على أهداف حيوية(*Schwarz,2013*)، و(الثانية) الاقتصاص ممن يهددون أمنها القومي، سواء كانت هجمات الخصوم تحاول بثّ تهديدات لينة تستهدف ثقافة الثورة الإسلامية وخطاطتها العقدية، أم تعد محاولة لزعزعة الأمن الوطني من خلال دعم المعارضة أو إضعاف النظام الإيراني ومؤسساته العسكرية، والأمنية، والسياسية، أو لكونها تنتظم ضمن سلسلة هجمات تستهدف خلخلة مشاريعها الاستراتيجية (النووية أو التسليحية)، و(الرابعة) تحقيق غاية ترتبط بالخطاطة العقدية للنظام الإيراني ومؤسسته الحوزوية والتي وجدت في هذا النمط من الممارسات تمهيداً لظهور الامام المهدي بعد فرض هيمنة إيران على أكثر من مجال من مجالات المواجهة مع قوى الشر، وعلى رأسها الشيطان الأكبر[238] (*Manshroo,2013*).

فبعد أن نجح الفايروس *Stuxnet* ومجموعة البرامج الخبيثة التي استنسلت بصمته البرمجية مثل *Flame*، و*DUQU* في بلوغ الطبقات العميقة من البرامج الإيرانية الاستراتيجية، توجهت إيران نحو التعجيل بعملية تطوير قدرات الردع السيبراني، وخلال بعد زمني قياسي، مع مباشرة عمليات تصعيدية وجهت دفة تأثيراتها على مؤسسات حيوية في الولايات المتحدة، وإسرائيل، كما لم تغيب دول خليجية، مثل السعودية، وقطر، والإمارات عن خارطة هجماتها الشرسة.

ويلاحظ تنوع هذه الهجمات، وتكاثر الجهات المشاركة فيها، بالإضافة الى انبساط مواردها على رقعة جغرافية تجاوزت الرقعة الجغرافية الفسيحة لإيران ذاتها. فعلى صعيد تنوع الهجمات نجد أن الهجمة التي استهدفت مؤسسات مالية أمريكية، وشركة أرامكو السعودية، وشركات نفطية حكومية كانت بواسطة فايروس إيراني الصنع أطلق عليه اسم *Shamoon*، بينما استخدمت تقنية رفض الخدمة في الهجمة التي استهدفت شركة *RASGAS* القطرية وكذلك الهجمات التي استهدفت مؤسسات مالية ومصرفية أمريكية، أو استخدام تقنيات تجسس رقمي متقدمة كما هو الحال عليه في الهجمتين الشهيرتين، زهرة الزعفران، وهجمة السطور خلال العامين 2013 و2014. كما أن التطور في التقنيات المستخدمة، وزيادة التعقيد في معمارية الهجمات السيبرانية قد فرض على الفصائل الإيرانية توظيف عدد كبير من قراصنة المعلومات، وترسيخ تحالفات واسعة لضمان نجاح الهجمات في إحداث تأثيرات جسيمة بالكيانات السيبرانية لخصوم إيران (هجمة الساطور).

أما بالنسبة لتعدد هوية المشاركين في الهجمات، فقد مورست هجمة الفايروس *Shamoon* بواسطة مجموعة قرصنة إيرانية أطلقت على نفسها "سيف العدالة القاطع"، وهي الجهة ذاتها التي مارست الهجمة على شركة الغاز القطرية، بينما قامت فصائل القسام السيبرانية بممارسة عمليات اكتساح المؤسسات المالية والمصرفية الأمريكية.

أما التوزع على الرقع الجغرافية، فلم يعد توطن قراصنة المعلومات والفصائل السيبرانية الإيرانية محصوراً بفضاء إيران السيبراني بعد أن استخدم مضيفات رقمية تعود الى جهات متعددة، وتقيم بعضها في فضاء خصومها، يضاف الى ذلك تكاثر أعداد الوكلاء السيبرانيين

---

[238] . عدّ قائد مقر عمليات الجيش الإيراني، بيهروز أسباطي، في تصريح له بتاريخ 20 أبريل عام 2012 ميدان الفضاء الافتراضي من أهم الوسائل للتحضير والتمهيد باتجاه ظهور الامام المهدي مصلح البشرية، والذي سيرسخ قواعد الحق، وينشر العدل بعد غيبته (*Manshroof,2013*).

لإيران في سوريا (الجيش الإلكتروني السوري)، وفي لبنان (فصائل حزب الله السيبرانية)، وفي غزة (فصائل عز الدين السيبرانية)، وفي اليمن (جيش اليمن السيبراني)، وفصائل أخرى تتوزع في بلدان أخرى، وفي قارات متعددة[239].

انتبه النظام الإيراني الى الخصائص الفريدة لفضاء النزاع السيبراني، ووجد فيه مناخاً مناسباً لمجالدة خصومه الذين قد تفوقوا عليه بقدراتهم التقنية وسطوتهم الحربية، بواسطة أدوات رقمية زهيدة الثمن، وبناء قدرات الموارد الوطنية بحيث تكون قادرة على مناكفة الخصوم، ومهاجمة كياناتهم السيبرانية الاستراتيجية، وإيقاع الأذى ببنيتها وخلخلة أدائها، دون الحاجة الى الولوج في ساحات الوغى التقليدية، حيث لا تستطيع الآلة العسكرية التي يمتلكها النظام مجاراة السطوة الغاشمة التي يمتلكها خصومه. يضاف الى هذا الأمر انفتاح فضاء الفيض السيبراني، وغياب الهوية الحقيقية في زحمة الكيانات المتكاثرة في فضائه المتخيّل، وتداخل عقد الارتباط في نسيجه الشبكاتي، ومغيب بصمة الحضور المكاني، الأمر الذي دفع بالنظام الى تطوير قدرات موارده البشرية، وتطوير آلة أدواته السيبرانية، وترسيخ تحالفات متينة مع قراصنة المعلومات من داخل إيران، وآخرين من خارجها، مع دعم بزوغ بؤر رقمية في المناطق الساخنة لاجتلاب أكثر ما يمكن من منافع مضافة الى قدراته السيبرانية.

وقد مرّت الخطاطة الإيرانية التي تبناها النظام الإيراني بسلسلة من المراحل، وبدأت بالنضج تدريجياً، وأخذت صبغة مميزة نتيجة للبصمة التي تميزت بها إيران، وطبيعة النهج الذي يتبناه النظام الإيراني، بالإضافة الى تكاثر أنماط التجاذبات وتنوع أشكال الضغوط التي سلطت على البلاد، من موارد شتى.

وكان حصيلة هذه التأثيرات مجتمعة بروز سمات مميزة، وأخرى فريدة التصقت بالتهديدات والهجمات التي تنطلق من فضاء إيران السيبراني، أو البؤر السيبرانية الموالية للنظام باتجاه خصومها التقليديين. ومن هذه الميزات، اعتماد إيران على قناتين لتوجيه مسارات هجماتها. وترتكز كل قناة من هاتين القناتين الى بنية تحتية للمعلومات والاتصالات تمارس نشاطها بمعزل عن الأخرى. وتستوطن القناة الأولى داخل حدود الفضاء السيبراني الملتحق بإيران، وتلتحق بفصائلها فرق ومجاميع إيرانية تتوزع بين المؤسسات العسكرية

---

[239] . دعمت إيران فصائل حزب الله اللبناني، والذي تصاعدت هجماته على الكيان الصهيوني في غضون المواجهات الشرسة التي اندلعت بلبنان عام 2006، وقد أسهم دعمها اللامحدود للفصائل السيبرانية للحزب، وحضورها السيبراني المباشر في كثير من الهجمات التي شنّت ضد الكيان الصهيوني في تطوير قدرات فصائله بحيث جذبت انتباه الولايات المتحدة مع بدايات عام 2008 وأسهمت في تنامي قلق الإدارة الأمريكية بعد نجاح حملة هذه الفصائل على مؤسسات التجارة والأعمال الصهيونية في عام 2012 (*Brunner,2015*).
كذلك هناك الكثير من الدلائل التي تؤكد تعاونها الوثيق ودعمها التقني واللوجستي للجيش السوري الإلكتروني *SEA* الذي نجح بتصعيد هجماته ضد أعداء النظام السوري، والذين يقيمون في خانة خصوم إيران، ونجح بإحداث تأثيرات ضارة في مواقع الكثير من وسائل الإعلام الأمريكية مثل: *The Washington Post, The Chicago Tribune, The Financia Times & Forbes* ، مع قرصنة نظم برمجية تعود الى كبريات الشركات الأمريكية العملاقة مثل: *Microsoft* (*Brunner,2015*). ولا يمكن تبرير التطور السريع في السطوة السيبرانية لفصائل هذا الجيش الإلكتروني إلا بوجود دعم تقني غير محدود من حليفة النظام السوري، إيران، التي أسهم دعمها المستمر في تطوير آلة الردع لدى هذه الفصائل مع حصول تطور ملموس في انتخاب الأهداف، وممارسة التهديدات والهجمات المتتالية على العدو المشترك للنظامين.
يضاف الى ذلك مسألة الولادة السريعة لجيش اليمن السيبراني التي تناغمت مع بدايات النزاع العسكري الذي اندلع بين ميليشيات الحوثي ودول التحالف العربي، مع بوادر ولادة ناضجة لكوادر خبيرة في ممارسة التهديدات والهجمات السيبرانية، لا نكاد نعثر عليها في الحفريات السيبرانية بفضاء اليمن السعيد؟.

إن الهجمات التي أعلنت عنها فصائل هذا الجيش الجديد، والتي شنّت على أهداف حيوية في المملكة العربية السعودية، شملت مواقع كل من وزارة الداخلية، والخارجية، والدفاع، بالإضافة الى مواقع أخبارية سعودية حصينة تؤكد وجود دعم من جهة متقدمة تقنياً في مجال حروب المعلومات، وحليفة حريصة على دعم ميليشيات الحوثيين الموالية للنظام الإيراني.

وتتبنى إيران في نهجها الدائم لاستنبات ودعم المزيد من الوكلاء السيبرانيين في أي بقعة تصلح لاستنهاض الرغبة في شن هجمات ضد خصومها التقليديين، سياسة التحريض والدعم غير المعلن، أو حتى مشاركة فصائلها السيبرانية تحت راية هؤلاء الوكلاء، مع حرصها الشديد على تغييب أي أثر من آثار الحضور أو الدعم، ومنح وكلاءها فرصة استعراض قدراتهم في اقتحام الحصون السيبرانية لأعدائها وخصومها السياسيين، مع توفير فضاء لنفي أي مساهمة مباشرة أو غير مباشرة في هذه التهديدات أو الهجمات متى أثير الغبار حولها.

والأمنية ومؤسسات بحثية وأخرى جامعية بالإضافة الى فرق قراصنة معلومات تناصر النظام أو تعمل بمعية مؤسسة الحرس الثوري الايراني، بينما تستوطن الثانية في فضاء معلوماتي يمتد على رقعة جغرافية واسعة خارج حدود إيران، ويلتحق بها فصائل من الوكلاء والحلفاء السيبرانيين للنظام الإيراني، ينتشرون في بلدان المنطقة، وبلدان نائية في مشرق الأرض ومغاربها، الأمر الذي يشكل تهديداً من نمط فريد، لأن كل قناة من هاتين القناتين تمارس هجماتها على خصومها، كما أن لكل منها بيئة حاضنة، وظروف تختلف عن الثانية بحيث تقلل من فرص تتبع مواردها، أو التنبؤ بأهدافها المحتملة، أو العثور على بصمات الفاعل الحقيقي في فضاء متخيل، تغيب عنه الحدود الجغرافية، وتغيّب هوية الجهات الفاعلة فيه وراء أقنعة رقمية مموهة (Kagan&Stiansen,2015).

ونجحت مؤسسة الحرس الثوري الإيراني في تصعيد آثار روح الانتماء لبلاد فارس وحضارتها العريقة في نفوس المواطنين الإيرانيين فدفعتهم الى ممارسة عفوية، وبدافع وطني، الى ممارسة الكثير من هجمات فضاء الفيض السيبراني، أو توجيه دقّة مهاراتهم (التي تلقنوها في أساليب وممارسات القرصنة لتجاوز عقبة الحظر الذي تمارسه الحكومة لشلّ أو كف تحركاتهم في فضاء الانترنيت الفسيح) لمهاجمة مواقع تستوطن في النسيج الشبكاتي للولايات المتحدة الأمريكية، أو دول غربية أخرى، متى استشعروا أن هناك ثمة نشاط قد يهدد كيان الأمة الإيرانية، متناسين خلافاتهم السياسية العميقة مع نظامهم، لأن قوة التصاقهم بتربة إيران، وتراثها، أشدّ بكثير من حدّة التناقض والنفرة التي تبعدهم عن الممارسات السياسية للثورة الإسلامية وخلافاتهم العميقة معها.

يضاف الى ذلك تثوير الخطاطة العقدية للمذهب الشيعي في نفوس الايرانيين، وولاؤهم المطلق له، مع عمق جذور غراس بذرة العشق الحسيني الذي يسكن في أرواحهم، لتجنيد جحافل من الشبيبة الإيرانية، وبصرف النظر عن انتمائها، أو معارضتها للنظام السياسي، الأمر الذي يزيد من عديد المتطوعين للقرصنة السيبرانية، ومهاجمة الخصم بهجمات رفض الخدمة، أو توظيف مهاراتهم لدرء كل ما قد يعتقدون أنه سيشكل خطراً على خطاطتهم العقدية، وتشعبات ارتباطاتها بممارساتهم الدينية، وولائهم لمبدأ الإمامة. وهو أمر لا نكاد نعثر عليه في كثير من دول المنطقة، وبقية بلدان الأرض.

ونبه الباحثان (Kagan&Stiansen,2015) (في المعهد الأمريكي لمشروع التهديدات الحرجة) الى سمة فريدة نشأت عن الاستراتيجية الفريدة التي تنتهجها إيران في إدارة دفة تهديداتها وهجماتها السيبرانية والتي تكمن في امتلاكها لمجموعتين متوازيتين من البنى التحتية التي تنطلق منها هذه التهديدات. الأولى: تستوطن ضمن نسيج البنية التحتية والاتصالية في إيران، أما الثانية: فتتوزع بين بلدان متعددة ومتباعدة وتعود الى وكلاء رقميين للنظام الإيراني قد تحالفت معهم لوجود مصالح وأهداف سياسية مشتركة، أو لتطابق الخطاطة العقدية، أو استأجرتهم للقيام بمهام محددة لتبعد نفسها عن دائرة اتهام خصومها.

وتشكّل هذه الاستراتيجية تهديداً من نمط جديد، حيث تسهم في تشتيت انتباه خصومها، وتفتّ عضدهم عند محاولة درء المخاطر المحتملة عن تهديداتها وهجماتها التي لا تتوفر دلائل قاطعة عن مصادر انطلاقها التي قد تتوزع بين مضيفات متعددة، ومواقع مختلفة، وخوادم تقيم بالولايات المتحدة، أو كندا، أو بلدان أوربية متعددة، أو مبرراتها التي قد تنشأ عن أمور قد لا ترتبط بصورة مباشرة

بالملف الإيراني ذاته بل ترتبط بملف نزاعات حزب الله بالمنطقة، أو الموجهة المستمرة بين حركة حماس والكيان الصهيوني، أو ملف المواجهة المستعرة بين الشرعية اليمنية والحوثيين، او خلاف تمتد جذوره الى ساحة النزاع في دول أمريكا اللاتينية[240] !.

وفي خضم هذا النشاط المحموم، الذي شمل بناء القدرات السيبرانية، وترسيخ البنى التحتية للمعلومات والاتصالات، وصياغة الاستراتيجية الدفاعية ـ الهجومية في فضاء البلاد السيبراني، وخارجه، حرص النظام الإيراني على إبقاء مؤسساته بعيدة عن الصراع المحتدم، وحاول أن يثبت صبغة الدفاع عن الحياض السيبرانية، دون ولوج النظام في دائرة ممارسة التهديدات والهجمات السيبرانية ضد خصومه، ليقلل من وطأة الضغوط المحتملة، من جهة، ويتجنب أي حصار قد ينال بنيته التحتية الاتصالية، أو حضوره السيبراني في فضاء الانترنيت العولمي.

بيد أن هذا السعي لم يكتب له النجاح نتيجة لوجود التجاذبات بين مؤسساته الأمنية والعسكرية، والعقدية، والسياسية، والتي تنطلق كل منها بتصريح يعبّر عن موقفها، بصرف النظر عن الموقف الذي يتبناه النظام، في كثير من الأحيان. الأمر الذي جعل هذه التصريحات تعاني من سمة التناقض والتباين، عندما تصدر عن هذه الجهة أو تلك، لوصف السطوة الإيرانية، وما نجحت بتحقيقه على أرض الواقع، أو عند الإعلان عن حصول هجمة رقمية على خصوم إيران.

من أجل هذا نجد الناطق بلسان الحكومة ينفي وجود قوة رقمية ضاربة ويقصر ممارسات إيران على زيادة حصانة نظم المعلومات والكيانات السيبرانية الإيرانية من الهجمات التي تمارس عليها بين الحين والآخر، وبين تصريحات يطلقها الناطق بلسان الحرس الثوري الإيراني، وآخر بلسان مؤسسة الباسيج، وثالث يصدع بلسان مؤسسة الدفاع المدني مؤكدين امتلاك إيران لقوة ردع رقمي، يتألف قوامها من قراصنة إيرانيين محترفين، يعملون بمعية الباسيج، بالإضافة الى مجاميع قرصنة مستقلة تنسّق عملها مع النظام الإيراني، وأن هذه الفصائل السيبرانية باتت قادرة على اختراق أنظمة الدفاع السيبراني والبنى التحتية للمعلومات والاتصالات لخصوم إيران والمتربصين بها، وإحداث تأثيرات موجعة في نسيجها الشبكاتي لدرء هجماتها المتكررة على فضاء إيران وكياناته السيبرانية الحيوية (*Mansharof,2013*). فتختلف من أجل ذلك نبرة التصريح ومدى مقاربته للواقع أو مجافاته له. وفي جميع الحالات تنزع التصريحات الى جهتين، (الأولى) تعبير عن الفخر بالقدرات السيبرانية الإيرانية التي ترعرعت في تربة ثقافة الثورة الإسلامية وتأكيد حصانة البلاد إزاء التهديدات مع امتلاك ذراع رقمي يمكن أن يمارس هجمات مؤثرة ضد أعداء إيران، ومهما كانت هويتهم. و(الثانية) تعبير عن التزام النظام الإيراني بنهج التقية العقدي، والتي يحرص من خلالها النظام عن ثني الأنظار عنه، وإبعاد شبهة مثل هذه الممارسات عنه، لإقصاء شبح العقوبات وآثار الحصار الذي أنهك البلاد.

وقد بالغ علي سعيدي، ممثل المرشد الأعلى في مؤسسة الحرس الثوري الإيراني، في تفاؤله بنتائج التحضيرات التي تعكف عليها المؤسسات الإيرانية، فاعتبرها تضاهي، الى حد كبير، الإجراءات التي تتبناها مؤسسات الإدارة الأمريكية، لا بل يمكن القول أن إيران قد سبقت الولايات المتحدة في مجال حروب المعلومات بشوط كبير، بحسب تصريحاته في شهر شباط من عام 2011.

---

240 . أظهرت التحليلات السيبرانية ـ الاستخباراتية، وتحليل أنماط أنشطة القرصنة السيبرانية التي مارستها كل من مجموعة *Parastoo*، وجيش فضاء إيران السيبراني، مجموعة القسام السيبرانية، خلال عام 2013، أن الهجمات التي مارستها هذه المجاميع الثلاثة تكاد أن تكون متقاربة في سماتها الى الحد الذي يوحي إما بوجود تنسيق عالي المستوى بين هذه الأطراف عند ممارسة الهجمات، أو أن هذه المجاميع ليست سوى هويات مصطنعة وتشكل حضوراً افتراضياً لكيان معلوماتي واحد، بات يعلن عن حضوره بأكثر من هوية رقمية (*HP,2014*).

وفي العام التالي ادعى إبراهيم جباري، قائد الحرس الثوري في مدينة قم، أن إيران تحتل المرتبة الثانية بين دول العالم على صعيد القدرات السيبرانية التي تتمتع بها في مجال حروب المعلومات، أما في عام 2013 فقد ذهب دفع محمد حسين، معاون سعيدي، الى القول أن إيران باتت تتبوأ المرتبة الرابعة على صعيد السلطان السيبراني بعد الولايات المتحدة، وروسيا، والصين (*Mansharof,2013*).

وبصرف النظر عن المبالغة، والنزعة الدعائية التي قد تستبطن مضامين هذه التصريحات، بيد أنه لم يعد من الممكن مدافعة حقيقة التطور المتسارع في قدرات إيران وسلطانها السيبراني في مجال ممارسة التهديدات السيبرانية وشنّ الهجمات السيبرانية على صعيد المنطقة، وضمن التراتبية العولمية.

ونلاحظ بداية هذه التصريحات عند نشوب النزاع مع المعارضة بعد اندلا ع الثورة الخضراء عام 2009، عندما أعلن علي سعيدي، ممثل المرشد الأعلى للثورة في مؤسسة الحرس الثوري الإيراني في شهر شباط من عام 2011، صراحة عن هوية انتماء جيش فضاء إيران السيبراني *ICA* عندما ذكر أنه يمارس مهامه في الفضاء السيبراني بالنيابة عن مؤسسة الحرس الثوري الإيراني. أدلى بهذا التصريح بعد نجاح الهجمة التي قامت بها فصائله على موقع صوت أميركا *VOA* الناطقة باللغة الفارسية، وعد نجاح هذه الهجمة رسالة صريحة الى وزيرة الخارجية الأمريكية، في ذلك التاريخ، هيلاري كلينتون، بحجم القدرات التي يمتلكها الحرس الثوري الإيراني في مجال حروب المعلومات، ومدى التقدم الذي تتمتع به فصائله السيبرانية، وأن هذه الهجمة هي ليست سوى رد على تجاوز الولايات المتحدة وتدخلاتها المستمرة في الشأن الداخلي الإيراني في دعمها للاحتجاجات المصاحبة للحركة الخضراء التي قامت بها المعارضة الإيرانية (*Mansharof,2013*).

كذلك نتلمس تصاعد حدّة التصريحات التي تنزع الى الإفصاح عن سطوة إيران السيبرانية بعد الآثار الوخيمة التي تسببت عنها هجمة الفايروس *Stuxnet* على مشروع نطنز النووي، لرفع معنويات الإيرانيين وبث الثقة في نفوس القيادات، بعد هذه الصدمة الموجعة.

فقد أعلن غلام رضا جليلي، رئيس مؤسسة المقاومة المدنية *Passive Resistance Organization*، بعد مدة قصيرة من حصول الهجمة، عن تأسيس مركز عمليات حرب المعلومات بالجمهورية الإسلامية *Cyber War Headquarters of The Islamic Republic of Iran* وذكر أنها ستقوم بمواجهة أعداء إيران المنتشرين في الفضاء السيبراني، وأن هذا المركز سيباشر بممارسة مهامه بالدفاع عن الحياض السيبرانية لإيران بإشراف مباشر من مؤسسة المقاومة السلبية (*MAI,2011*).

كما أكّد في تصريح آخر على أن هجمة الفايروس الخبيث *Stuxnet* قد عززت التنسيق المشترك بين جميع المؤسسات الأمنية في إيران، وبحضور مكثف لمؤسسته ووزارة المخابرات الإيرانية، ومؤسسة الحرس الثوري الإيراني، والهيئات القضائية لتسخير جميع الإمكانيات المتاحة بالبلاد للارتقاء بالكفاية الأمنية لالفضاء السيبراني الإيراني، وترسيخ حصانته ضد أية هجمات محتملة بالمستقبل القريب (*MAI,2011*).

كذلك لم يفلح في إخفاء الرغبة المحمومة لمؤسسته بتجنيد قراصنة المعلومات واستقطابهم لدرء الأخطار عن فضاء إيران السيبراني ومهاجمة مصالح الدول المعادية لإيران، فدعا في كلمة له ألقاها، خلال المؤتمر الثاني الذي عقدته مؤسسته خلال النصف الأول من عام 2011 ذوي النوايا الحسنة من قراصنة المعلومات، الذين ينتمون الى روح الثورة الإسلامية، ببذل كل ما في وسعهم من خلال

تسخير قدراتهم وخبراتهم لدعم أهداف الجمهورية الإسلامية وتعزيز سلطانها السيبراني. كما حذّر قراصنة المعلومات الذين يرومون الأضرار بالمواطنين الإيرانيين، أو بمكتسبات الثورة الإسلامية، لأنهم لن يفلتوا من قبضة المراقبة الصارمة لمؤسسته، وأن هناك ثمة إجراءات مشددة، وعقوبات صارمة لن يستطيعوا الإفلات منها (*MAI,2011*).

وذهب علي فاضلي، المدير التنفيذي لمؤسسة الباسيج، الى تبرير ممارسات قراصنة المعلومات الذين يعملون بمعية مؤسسته لأن هجماتهم تستهدف مواقع ويب يستخدمها أعداء إيران لشن حرب ناعمة ضد الثورة الإسلامية في إيران، كما أن مشاركتهم الفاعلة تساهم في ضمان حماية أمن معلومات الفضاء السيبراني بالبلاد من حملات التشويه. ثم عاد وأكد أن مؤسسة الباسيج تعمل جاهدة ومن خلال الدعم الذي تقدمه الى قسم تقنية المعلومات والاتصالات الملحق بها لمواجهة التهديدات السيبرانية المتزايدة التي تستهدف إيران في أكثر من مجال من مجالات حروب المعلومات، وأنه لولا هذه الجهود الحثيثة فإن إيران لن تكون قادرة على درء التهديدات المتلاحقة على بنيتها التحتية وأمنها السيبراني الوطني. وقد شدد على الدور المهم الذي يمارسه الجيش السيبراني الذي يعمل مع مؤسسة الباسيج، والذي يتألف من مجموعة من أساتذة الجامعة، والطلبة المتميزين بالمؤسسة الجامعية والحوزات العلمية، ممن نذروا قدراتهم وخبراتهم السيبرانية لدرء الأخطار المحدقة بإيران من أعدائها (*MAI,2011*).

من جهة أخرى، تصرّ شريحة أخرى من الإدارات الحكومية الإيرانية على عدم امتلاك إيران سوى قدرات رقمية دفاعية لدرء آثار التهديدات والهجمات السيبرانية التي باتت تمارس بكثافة ضد إيران، وأن ما تتناقله الولايات المتحدة وحلفاؤها بصدد امتلاك إيران قدرات ردع رقمي جزء لا يتجزأ من الاتهامات التي تلفّق ضد الثورة الإسلامية لتشويه سمعتها في المجتمع الدولي، ولتبرير شن المزيد من الهجمات السيبرانية الشرسة ضد كياناتها السيبرانية وبنيتها التحتية (*Mansharof,2013*).

وقد تصدر التصريحات في بعض الأحيان، بصورة غير مباشرة، مثل التصريح الذي أطلقه بيروز كماليان لإبعاد شبهة انتماء مجموعة *Ashiyane* الى الحرس الثوري عندما أعلن أن مجموعته تمارس هجماتها ضد خصوم النظام، داخل إيران وخارجها، وأكد أن مجموعته تعمل بصورة مستقلة في شن هجماتها ضد أهداف الجهات المعادية لإيران (*Mansharof,2013*).

بينما تصدر تصريحات مباشرة، في أحيان أخرى، عبر القنوات الحكومية مثل التصريح الذي أدلى به الناطق بلسان وزارة الخارجية الإيرانية (بعد الهجمات الواسعة التي اكتسحت عدد كبير من المؤسسات المالية في مدينة نيويورك، واتهمت الإدارة الأمريكية مساهمة النظام الإيراني في دعم هذه الهجمة) وأعلن أن إيران لم ولن تقوم بأي نشاط هجومي في فضاء الفيض السيبراني قد ينشب عنه آثار ضارة أو تخريبية في الكيانات السيبرانية للغير، كما أنها لم تدعم هذه الهجمات بصورة غير مباشرة، أو مباشرة، وأن الاتهامات الأمريكية تفتقر الى المصداقية، وأنها جزء من الاستهداف الدائم لإيران (*AFP,2016*).



مصادر الدراسة

مصادر الدراسة

المصادر العربية:

1. أتزو، سون، (2010)، **فن الحرب**، ترجمة وتقديم أحمد ناصيف، الطبعة الأولى، دار الكاتب العربي، بيروت
2. آل غور، (2015)، **المستقبل: ستة محركات للتغيير العالمي**، ترجمة عدنان جرجس، سلسلة عالم المعرفة، العدد 423، المجلس الوطني للثقافة والفنون والآداب، الصفاة، الكويت.
3. حمدان، محمد، (2010)، **الحرب الناعمة**، دار الولاء، بيروت، لبنان.
4. الرزو، حسن مظفر، (2008)، **المواجهة غير المعلنة بين حزب الله والكيان الصهيوني في الالفضاء السيبرانيي للانترنيت**، **مجلة المستقبل العربي**، المجلد الثلاثون، العدد 342، آب 2007/8، الصفحات 15-35، مركز دراسات الوحدة العربية، بيروت، لبنان.
5. الزين، حسن، و ب. عاصي، (2011)، **الحرب الناعمة: المفهوم ـ النشأة ـ وسبل المواجهة**، سلسلة الندوات الثقافية، مركز قيم للدراسات الثقافية، بيروت، لبنان.
6. سعودي، الدكتور محمد عبد الغني، (2010)، **الجغرافية السياسية المعاصرة: دراسة الجغرافية والعلاقات السياسية الدولية**، مكتبة الأنجلو مصرية، القاهرة، مصر.
7. سلطان، الدكتور جاسم، (2013)، **الجغرافيا والحلم العربي القادم**، الجزء الثامن، مشروع النهضة، سلسلة أدوات القادة، تمكين للأبحاث والنشر، بيروت، لبنان.
8. عبد السلام، رفيق، (2008)، **الولايات المتحدة بين القوة الصّلبة والقوة الناعمة**، العدد 6، أوراق الجزيرة، المركز الجزيرة للدراسات، الجزيرة، الدوحة، قطر.
9. العيسوي، الدكتور فايز محمد، (2000)، **الجغرافيا السياسية المعاصرة**، دار المعرفة الجامعية، القاهرة، مصر.
10. مركز الحرب الناعمة للدراسات، (2014)، **الحرب الناعمة: معالم رؤية الامام الخامنئي**، الطبعة الأولى، مركز الحرب الناعمة للدراسات، بيروت، لبنان.
11. مركز الحرب الناعمة للدراسات، (2014)، **مدخل الى الحرب الناعمة**، الطبعة الأولى، مركز الحرب الناعمة، بيروت، لبنان.
12. مركز قيم للدراسات، (2011)، **رؤية الامام خامنئي في مواجهة الحرب الناعمة**، سلسلة الندوات الفكرية، الطبعة الأولى، مركز قيم للدراسات، بيروت، لبنان.
13. ناي، ج.، (2004)، **القوة الناعمة ـ وسيلة النجاح في السياسة الدولية**، ترجمة الدكتور محمد توفيق البجيرمي، الطبعة الأولى، 2007، العبيكان للنشر، الرياض، السعودية.

المصادر الأجنبية:

1. A.P.,(2014), **Tarh Andishan: The New Cyber Threat Comes From Iran**, STI News, Dec. 20th 2014.
2. AA, (2005), **An Internet Revolution in Qom's Religious Establishment**, Al-Sharq Al-Awsat, on Friday, 17th June, 2005.
3. Abadpour, A., & C., Anderson, (2013), **Fights, Adapts, Accepts: Archetypes of Iranian Internet Use**, Iran Media Program, Annenberg School for Communication, University of Pennsylvania, USA.
4. Abbasi, A., Niaraki, A., & B., Dehkordi, (2008), **A review of ICT status and development strategy plan in Iran**, International Journal of Education and Development using Information and Communication Technology (IJEDICT, Vol. 4, Issue 3, pp. 143-154.
5. Advocacy, (2015), **New Research: Iran is Using Intelligent Censorship on Instagram**, Global Voices, 7 May 2015.
6. AFP, (2016), **Iran Denies Backing Cyber Attacks On US after Indictments**, The Times of Israel, March 2016.
7. Aghili, S., & Kahnegi, F., (2013), **A Domestic Model to Counter the Cyberspace Threats in Iran**, International Journal of Business and Social Science , Vol. 4 No. 7; July 2013.
8. Aitel, D., (2015), **Iran Is Emerging As One Of The Most Dangerous Cyber Threats To The US**, Military & Defense, Available At: http://Www.Businessinsider.Com/Defense.
9. Akamai, (2014),**The State of the Internet / Q3 2014**, www.stateoftheinternet.com.
10. Akl, A., (2013), **Iran Plans its own Internet with Chinese Help**, VOA News, July 31st 2013, Available At: http://www.voanews.com/section/middle_east/2206.html.
11. Alavi, N., (Editor), (2005), **We Are Iran: The Persian Blogs**, Soft Skull Press, Inc., Brooklyn, New York, USA.
12. Alimardini, M., Jacobs, F., & E., Biddle, (2015), **Iran is Using "Intelligent" Censorship on Instagram**, Free Expression, https://advox.globalvoices.org/.
13. Allison, R., (2008), **Russia Resurgent? Moscow's Campaign to "Coerce Georgia to Peace**", International Affairs, Vol. 84, No. 6, pp. 1145–71.
14. Ameri, R., (2014), **Higher Education and Quality Assurance in Iran: A Brief Survey**, Ministry of Science, Research and Technology (MSRT), Tehran, Iran.
15. Ameri, R., (2014), **Higher Education and Quality Assurance in Iran: A Brief Survey**
16. Amir-Ebrahimi, M., (2010), **Blogging from Qom, behind Walls and Veils**, Project Muse, Scholarly Online Journal.
17. Andress, J., Winterfield, S., & L., Ablon, (2014), **CYBER WARFARE: Techniques, Tactics and Tools for Security Practitioners**, SECOND EDITION, Technical Edition, Elsevier, Amsterdam, Holland.
18. Anoosheh, E., (2012), **Counter Measurements of the Islamic Republic of Iran**, ECIW 2012, 11th European Conference on Information Warfare and Security.
19. Arquilla, J. & D., Borer, (Editors), (2007), **Information Strategy and Warfare: A Guide to Theory and Practice**, Routledge &Francis, New York, USA.

20. Aryan, S., Aryan, H., & J. Halderman, (2013), **Internet Censorship in Iran: A First Look**, Proceedings of the 3rd USENIX Workshop on Free and Open Communications on the Internet, August 2013.
21. Atashak, M., & P., Mahzadeh, (2008), **E-government Status in Iran (TAKFA Plan Case Study),** World Applied Sciences Journal 4 (Supple 2): 12-20, 2008.
22. Azani, E., (2015), **Cyber-Terrorism Activities**, Report No.4, ICT Cyber Team Review, ICT Cyber-Desk Team, International Institute for Counter-Terrorism (ICT), Israel.
23. Baggili, I., (Ed.), (2010), **Digital Forensics and Cyber Crime**, Second International ICST Conference, ICDF2C 2010, Abu Dhabi, United Arab Emirates, October 4-6, 2010.
24. Bailly, J., (2012), **The Impact of Social Media on Social Movements: A Case Study of the 2009 Iranian Green Movement and the 2011 Egyptian Revolution**, Department of Political Science, College of Liberal Arts, Washington State University.
25. Baker, J., (2015), **Iran: The Cyber Nation – Timeline of Every Hack**, XPAT Nation, Available at: http://xpatnation.com/.
26. Barducci, A., (2011**), Iran Preparing Serious Cyber Attack Against the U.S. from Latin America**, International Policy Council, Dec., 14th 2011.
27. BBC, (2009), **'Iranian Cyber Army' Hits Twitter**, BBC News, December, 18th, 2009.
28. BBC, (2013), **Structure of Iran's Cyber Warfare,** The BBC Persian.
29. Beaumont, C., (2010), **Baidu hacked by Iranian Cyber Army**, The Telegraph, http://www.telegraph.co.uk/.
30. Behrouzan, O.,(2005), **Persian Blogs Against "The Dual Language", Knowledge Exchange,** February 2005.
31. Berkeley, B., (2006), **Bloggers vs. Mullahs: How the Internet Roils Iran**, World Policy Journal , Spring 2006.
32. Berman, I., (2013), **The Iranian Cyber Threat Revisited, U.S. House of**
33. Berman, I., (2013), **The Iranian Cyber Threat, Revisited, Statement before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Cybersecurity**, Infrastructure Protection, and Security Technologies, March 20, 2013.
34. Bertelsmann, S., (2012), **BTI 2012 - IRAN Country Report**, Gütersloh: Bertelsmann Stiftung.
35. Bertelsmann, S., (2014), **BTI 2014 – IRAN Country Report**, Gütersloh: Bertelsmann Stiftung.
36. Bicchirea, L., (2015), **There's Evidence the 'Yemen Cyber Army' Is Actually Iranian**, The Vice Channel, Vice Media LLC.
37. Bilbao-Osorio, B., Dutta, S. & B., Lanvin, (2014), **The Global Information Technology Report 2014: Rewards and Risks of Big Data**, Insight Report, World Economic Forum
38. Bilbao-Osorio, B., Dutta, S., & B., Lanvin, (Editors), (2013), **The Global Information Technology Report 2013 Growth and Jobs in a Hyper-connected** , Insight Report, World Economic Forum, Geneva.
39. Bilbao-Osorio, B., Dutta, S., & B., Lanvin, (Editors), (2014), **The Global Information**
40. Bilbao-Osorio, B., Dutta, S., Geiger, T., & B., Lanvin, (2014), **The Networked Readiness Index 2013: Benchmarking ICT Uptake and Support for Growth and Jobs in a Hyperconnected World**, World Economic Forum.
41. Billo, C., & W., Chang, (2004), **Cyber Warfare: An Analysis Of The Means and Motivations of Selected Nation States,** Institute For Security Technology Studies, The Dartmouth College, Hanover.
42. BMI, (2015), **Sanction Easing Benefits Iran's E-Commerce and Consumer Electronics Markets in Iran**, Multiple Industries, BMI Research, Tue May 05, 2015.

43. Bollier ,D.,(2003), **The Rise Of Netpolitik : How the Internet Is Changing International Politics and Diplomacy** ,A Report of the Eleventh Annual Aspen Institute, Aspen Institute, Washington D.C., USA.
44. Borna, T., & A., Seifloo,, (2015), **Electronic Government, Its Environmental and Social Effects: Case of Iran**, TMMOB, Planlama:24 (3):131-138.
45. Bowen, K., & J., Marchant, (2014), **Revolution Decoded: Iran's Digital Landscape,** Small Media Organization, smallmedia.org.uk.
46. Boyce, B., (2010), **Iranian Government Encourages Piracy,** Neowin, Available At: http://www.neowin.net/.
47. Boyle ,A.,(2009), How Iran's Internet Works, MSN, Cosmic LOG, Thursday, June 18, 2009.
48. Bozorgmher, N., (2014), **Iranian e-Commerce Thrives Despite Obstacles**, Available At: http://www.ft.com/world/mideast/iran.
49. Bradley, M,(2007), **Political Islam, Political Institutions and Civil Society in Iran: A Literature Review,** International Development Research Centre (IDRC) , July 2007
50. Brunner, J., (2015), **Iran Has Built an Army of Cyber-Proxies**, The Tower Magazine, Issue 29, 2015.
51. Bunt, G., (2009), **iMuslims: Rewiring the House of Islam**, The University of North Carolina Press, Chapel Hill, USA.
52. Carafano, J.,(2009), **All a Twitter: How Social Networking Shaped Iran's Election Protests**, Backgrounder, No. 2300, July 20, 2009.
53. Carr, J., (2010), **Inside Cyber Warfare**, O'Reilly Media, Inc., California, USA.
54. Carr, J., (2012), **Inside Cyber Warfare**, Second Edition, O'Reilly Media, Inc., California, USA.
55. Center For Global Communication Studies, Annenberg School For Communication, University Of Pennsylvania.
56. Chandramouli, R., & S., Rose, (2013), **Secure Domain Name System (DNS) Deployment Guide**, NIST Special Publication 800-81-2, National Institute of Standards and Technology, U.S. Department of Commerce,
57. Chopitea, T., (2012), **Threat Modelling of Hacktivist Groups, Organization, Chain of Command, and Attack Methods**, Master of Science Thesis in Secure and Dependable Computer Systems, Chalmers University of Technology University of Gothenburg, Department of Computer Science and Engineering, Göteborg, Sweden.
58. Cilluffo, F., Cardash, S.,& G., Salmoiraghi, (2012), **A Blueprint for Cyber Deterrence Building Stability through Strength**, Military and Strategic Affairs ,Volume 4 ,No. 3, December 2012.
59. Cilluffo, K., (2012),**The Iranian Cyber Threat to the United States**, The George Washington University, USA.
60. Cilluffom F., (2013), **Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure**, The Homeland Security Policy Institute, The George Washington University, USA.
61. CIMA, (2009), **A Guide to New Media in Iran**, Center for International Media Assistance, USA.
62. Cobos, A., (2012), **Nodes and Codes: The Reality of Cyber Warfare**, School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas, USA.
63. Cohen, D., & A., Rotbart, (2013), **The Proliferation of Weapons in Cyberspace**, Military and Strategic Affairs, Volume 5, No. 1, May 2013.

64. Cohen, E., & B., Krishnamurthy, (2009), **A Short Walk in the Blogistan**, AT&T Labs–Research, New Jersey.

65. Cohen, M., Freilich, H., & G., Siboni, (2015), **Israel and Cyberspace: Unique Threat and Response**, International Studies Perspectives (2015) 0,1–15.

66. Cohen-Almagor, R., (2012), **In Internet's Way: Radical, Terrorist Islamists on the Free Highway**, International Journal of Cyber Warfare and Terrorism, 2(3), 39-58, July-September 2012.

67. Colarik, A., (2006), **Cyber Terrorism: Political and Economic Implications, IDEA Group Publishing**, London UK.

68. Connell, M., (2014), **Deterring Iran's Use of Offensive Cyber : A Case Study**, Analysis & Solution, CAN, USA.

69. Conrad, D., (2000), **A Quick Introduction to the Domain Name System**, Nominum Inc., USA.

70. Constantin, L., (2014), **Iranian Hackers Compromised Airlines, Airports, Critical Infrastructure Companies**, PC World, Dec. 2nd 2014.

71. Constantin, L., (2015), **Iranian Cyberespionage Group Attacked Over 1,600 High-Profile Targets in One Year**, Security News, Available At: http://www.csoonline.com/.

72. Conway, M., (2003), **Cyber Cortical Warfare: The Case of Hizbollah.org**, Paper prepared for presentation at the European Consortium for Political Research (ECPR) Joint Sessions of Workshops, Edinburgh, UK, 28 March – 2 April, 2003.

73. Crowdstrike, (2014), **Global Threat Intel Report**, CrowdStrike, Avialable At: www.crowdstrike.com.

74. Crowdstrike, (2015),**2015 Global Threat Report**, The Intelligence Team, Crowd Strike, USA.

75. CTNS, (2016), **Current Capabilities and Emerging Threats**, Strategic Primer: Cybersecurity, Volume 2, Spring 2016.

76. Czosseck, C., & K., Geers, Editors,(2010), **The Virtual Battlefield: Perspectives On Cyber Warfare**, IOS Press, Washington, USA.

77. Daniel Cohen, D., & A., Rotbart, (2013), **The Proliferation of Weapons in Cyberspace**, Military and Strategic Affairs ,Volume 5 , No. 1 ,May 2013.

78. Dareini, A., (2012), **Iran: 'Flame' Virus Fight Began with Oil Attack (Update),** PHYS. ORG., 30 May 2012.

79. Dareini, A., (2014), **Report: Iran Court Orders Instagram Blocked**, Phys.Org.

80. Davarinejad, M., & M., Saffari, (2010), **Iran: .ir**, Digital Review of Asia Pacific 2009–2010.

81. DeNardis, **L., (2015), Internet Architecture as Proxy for State Power,** IP Justice Journal, August 15, 2015.

82. Deutch, J.,(1996), **Statement Before the US Senate Governmental Affairs Committee ,(Permanent Subcommittee on Investigations)**, June 25. Available online at http://www.nswc.navy.mil/ISSEC/Docs/Ref/InTheNews/fullciatext.html .

83. DoD, (2002), **Department of Defense Dictionary of Military & Associated Terms**, U.S. Navy, USA.

84. Dodrill, T., (2015), **Bowman Avenue Dam Breached By Iranian Cyber Hackers**?, INQUISTIR, Dec., 21ST ,2015.

85. Douglass, W., (2012), **21st Century Cyber Security: Legal Authorities and Requirements**, Strategy Research Project, United States Army War College, USA.

86. Drezner **, D. &** H. Farrellm, (2004), **The Power And Politics Of Blogs,** George Washington University, July 2004.

87. Dudley, N., (2015) , **Iran is Ready for an E-commerce Boom**, Agah Group, Available At: http://agahgroup.com/.
88. Dutta, S., & B., Bilbao-Osorio, (Editors), (2012), **The Global Information Technology Report 2012: Living in a Hyperconnected World**, World Economic Forum, Geneva.
89. Dutta, S., Geiger, T., & B., (Editors), (2015), **The Global Information Technology Report 2015: ICTs for Inclusive Growth**, Insight Report, World Economic Forum, Geneva.
90. Edge Wave, (2015), **Nation States: Why They Hack: China North Korea Russia Iran Israel United States, Motivations That Drive Nation States to Participate in Cyber Activity**, Edge Wave, USA.
91. Eist, (2014), **World's Top 10 Countries with Slow Internet Connection**, Connection, Elist10, http://www.elist10.com/worlds-top-10-countries-slow-internet-connection/.
92. EIU, (2004), **Iran: Telecoms and technology, Market profile, Telecoms and Technology Forecast World: Main Report**, The Economist Intelligence Unit.
93. **Electronic Government in Iran: A Case Study**, Online Journal of Social Sciences Research, Volume 2, Issue 9, pp 254-262; October, 2013.
94. Erbschloe, M., (2001), **Information Warfare: How to Survive Cyber Attacks**, Osborne/McGraw-Hill, New York, USA.
95. ESCWA, (2005), **Information Society Indicators**, E/ESCWA/ICTD/2005/1**,** Economic and Social Commission for Western Asia, United Nations, New York, USA.
96. Esfandiary, D., & and A., Tabatabai , (2015), **Iran's Cyberattacks Are Likely To Increase. Here's Why**,The Washington Post, November 18, 2015.
97. Even, S., & D., Siman-Tov, (2012),**Cyber Warfare:** Concepts and Strategic Trends, INSS, Institute for National Security Studies, Memorandum No. 117, May 2012.
98. Evron, G., (2009), **The Iranian 'Proxy War'**, Available At: http://www.darkreading.com/risk/the-iranian-proxy-war/d/d-id/1131397
99. F.H, (2015), **Iran: Freedom on The Net-2015**, Freedom House.
100. Faris, R. & R., Villeneuve, (2008), **Measuring Global Internet Filtering**, In Deibert, R.J., Palfrey, J.G., Rohozinski, R. & Zittrain, J. (Eds.), Access Denied: The Practice and Policy of Global Internet Filtering, Cambridge: MIT Press.
101. FARS, (2013), **Iran to Display 12 New Home-Made Cyber Products Saturday**, FARS News Agency, Sat Dec 14, 2013 2:50.
102. Farwell, J., & R., Rohozinski, (2011), **Stuxnet and the Future of Cyber War**, Survival, Vol. 53 no. 1, February–March 2011, pp. 23–40.
103. Fatemi, O., (2012), **Overall Policy and Coordination section : Iran Report** , Report On Information Policies Indicators In Asia, Tehran, Iran.
104. Finkelstein, C., & K., Govern, (2015), **Introduction: Cyber and the Changing Face of War**, Faculty Scholarship. Paper 1566, Penn Law: Legal Scholarship Repository, University of Pennsylvania Law School.
105. Finkle, J., (2011), **Factbox: Cyber Warfare Expert's Timeline for Iran Attack**, Reuters, Dec., 2nd 2011.
106. FRD, (2012), **Iran's Ministry of Intelligence & Security: A Profile**, A Report Prepared by the Federal Research Division, Federal Research Division Library of Congress, Washington, D.C., USA.
107. Freedom House, (2015), **Freedom on The Net 2015: Iran**, www.freedomhouse.org.
108. FWC, (2014), **Computer Crimes in Iran: Online Repression in Practice**, Article 19, Free Word Centre, London, UK.

109. FWC, (2015), **Computer Crimes in Iran: Risky Online Behaviour 2015**, Article 19, Country Report, Free World Center, London, UK.

110. Ghasimi, R., (2012), **Economy of Iran under Fourth and Fifth Five-year Development Plans**, Money and Economy, Vol. 7, No. 1, Fall 2012.

111. Ghorbani, M., Sadeghzadeh, A., & A., Nagafgholinejad, (2015), **Cooperation Programs In IRAN On The Context Of Technology, To Access, Develop And Transform Of Information**, IFLA, WLIC-2015, Cape town.

112. Giacobino, L., Abadpour, A., Anderson, C., Petrossian, F., & C., Nellemann, (2014), **Whither Blogestan: Evaluating Shifts In Persian Cyberspace**, Iran Media Program

113. Gill, T., & P., Ducheine, (2013), **Anticipatory Self-Defense in the Cyber Context**, Volume 89, International Law Studies, US Naval War Studies, USA.

114. Globalist, (2014), **Ten Facts: Iran & the Internet, Can the Reform government in Iran Finally Bring the Country's Internet Up to Speed?**, The Globalist, March 18, 2014.

115. Godwin, H., (2014), **East-West Institute, Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity**, Policy Report 2/2014.

116. Green, J., (Editor), (2015), **Cyber Warfare: A Multidisciplinary Analysis**, Routledge, Francis & Tylor Group, New York, USA.

117. Grewatz, R., (2013), **Analysis of Stuxnet and Issues in Cyber-Warfare**, CS 111

118. Grobman, S., (2016), **Iranian Hacker Indictment Reminds US That Risks to Critical Infrastructure Are Real**, Available at: http://www.darkreading.com/partner-perspectives/intel/iranian-hacker-indictment-reminds-us-that-risks-to-critical-infrastructure-are-real/a/d-id/1324843

119. Habibi, N., (2014), **Iran's Over-education Crisis: Causes and Ramifications**, Middle East Brief, Crown Center for Middle East Studies, Brandeis University.

120. Hacker5, (2013), **Iran, The World's Largest Cyber Army!**, Available at: http://www.hackers5.com/

121. Hackmageddon, (2016), **Information Security Timelines & Statistics**, Available at: http://www.hackmageddon.com/2016/03/24/february-2016-cyber-attacks-statistics/.

122. Hanna, R.,(2006), **Jihadism Online - A Study Of How Al-Qaida And Radical Islamist Groups Use The Internet For Terrorist Purposes** , FFI/RAPPORT-2006/00915, Forsvarets Forskningsinstitutt, Norwegian Defense Research Establishment , Norway.

123. Harris, S., (2014), **Forget China: Iran's Hackers Are America's Newest Cyber Threat**, The Complex, Feb., 14th, 2014.

124. Hathaway, D., (2011), **The Digital Kasserine Pass: The Battle Over Command and Control of DoD's Cyber Forces**, 21st Century Defense Initiative, Foreign Policy, Brookings, USA.

125. Hegazy, I., (2012), **Triangle of Middle East Cyber Warfare: Egypt-Israel-Iran**, Cairo Security Camp,2012, Cairo, Egypt.

126. Hemmat, A., & R., Ellett, (2011), **Cyber Warfare (Russia, China, Iran)**, Department of Political Science, Beloit College, May 5, 2011.

127. HITCON, (2013), **A Comparative Study: Iran, Russia & China Cyber Conflict**, RSA Conference, Europe 2013, July, 19th 2013.

128. Holler, J., (2015), **Who or What is Tarh Andishan and Why Should We Care**, PULSE, LinkedIn, July 13th 2015.

129. HP, (2014), **Companion to HPSR Threat Intelligence Podcast Episode 11 Threat Intelligence Briefing,** Episode 11, February 2014, HP Security Research, USA.

130. HP, (2014), **Companion to HPSR Threat Intelligence Podcast Episode 11 Threat Intelligence Briefing**, Episode 11, February 2014, HP Security Research, USA.
131. HP, (2015), **Cyber Risk Report 2015**, HP Security Research, Heleiwet Packard, USA.
132. HPSR, (2015), **HP Cyber Risk Report 2015**, HP Security Research, Heleiwet Packard, USA.
133. Hwang, J., (2012), **China's Cyber Warfare: The Strategic Value of Cyberspace and the Legacy of People's War**, Ph.D., Thesis, School of Geography, Politics and Sociology, University of Newcastle upon Tyne.
134. I.I.S, (2015), **ICT Facts & Figures, Measuring IRAN Information Society**, IRAN Information Society, Tehran, IRAN.
135. I.I.S., (2015), **Facts & Figures: Iran Information Society- 2015**, Measuring the Information Society of Iran, Information Technology organization of Iran, Ministry of ICT, Tehran, Iran.
136. I.P, (2012), **General Jalali: "Iran Has Begun to Operate Its First Cyber Army**, The Iran Political Analysis Project, Iran Politik, Feb. 21st 2012.
137. I.T.I.C, (2006), **Terrorism and Internet: Hezbollah's Widespread Use Of The Internet as A Means to Distribute Anti-Israeli, Anti-Jewish, and Anti-American Incitement as Part of The War for The Hearts and Minds** (as at December 3, 2006), Intelligence and Terrorism Information Center, Center for Special Studies (C.S.S), Tel Aviv, Israel.
138. I.T.O., (2015), **ICT Monitoring System for Iran**, Information Technology Organization of Iran, 2nd Edition, Tehran, May 2015.
139. I.T.O.I., (2013), **ICT Economic Indicators in I.R. of Iran**, Information Technology organization of Iran, Ministry of ICT, Tehran, Iran.
140. I.T.O.I., (2014), **Content of Network Resources in I.R. of Iran**, Information Technology organization of Iran, Ministry of ICT, Tehran, Iran.
141. IBP, (2011**), IRAN; Country Study Guide, Volume 1: Strategic Information & Development**, Global Investment & Business Center, Washington D.C., USA
142. ICHR, (2014), **Internet in Chains: The Front Line of State Repression in Iran**, International Campaign for Human Rights in Iran, http://www.iranhumanrights.org/.
143. ICHR, (2015), **Official Claims Smart Internet Filtering Overblown**, International Campaign for Human Rights in Iran.
144. ICIT, (2015), **Know your Enemies, A Primer on Advanced Persistent Threat Group**, Institute for Critical Infrastructure Technology, November,2015.
145. ICRTC, (2005), **A Report on the Status of the Internet in Iran**, Iran CSOs Training & Research Center.
146. ICT, (2014), **Cyber-Terrorism Activities: Report No. 4**, ICT CyberDesk Review, International Institute for Counter Terrorism, Tel Aviv, Israel.
147. ICTRC,(2005), **A Report on the Status of the Internet in Iran**, Iran CSOs Training & Research Center, http://www.genderit.org/upload/ad6d215b74e2a8613f0cf5416c9f3865/
148. IDC, (2013), **Cyber-Terrorism Activities Report No. 4**, ICT Cyber-Desk Review, IDC Herzliya, Institute for Counter-Terrorism, Israel.
149. IDC, (2014), **Cyber-Terrorism Activities Report No. 5,** ICT Cyber-Desk Review, IDC Herzliya, Institute for Counter-Terrorism, Israel.
150. IDF, (2006), **Terrorism & Internet: Hezbollah's Widespread Use of The Internet as A Means To Distribute Anti-Israeli, Anti-Jewish & Anti-American Incitement as**

Part of the War for The Hearts & Minds, Intelligence & Terrorism Information Center, The Center of Special Studies, Israel.

151. IDF, (2008), **The Internet & Terrorism: Aqsa Tube, Intelligence & Terrorism information Center**, Israeli Intelligence Heritage & Commemoration Center, IDF, Israel.
152. IDR, (2013), **Zeros and Ones: Tackling Cyber at The Tactical Edge**, IHS Jane's International Defence Review, Nov., 5th 2013.
153. IFR, (2013), **Zeros And Ones: Tackling Cyber at The Tactical Edge**, IHS Jane's International Defence Review, Nov. 5th 2013.
154. IHRC,(2009), **Ctrl+Alt+Delete: Iran's Response to the Internet**, Iran Human Rights Documentation Center, New Haven, Connecticut.
155. IHRO, (2014), **Internet in Chains: The Front Line of State Repression in Iran**, International Campaign for Human Rights in Iran, Iran Human Rights Organization, www.iranhumanrights.org.
156. IICT, (2013), **Cyber-Terrorism Activities**, Report No. 5, ICT Cyber Desk, International Institute of Counter Terrorism, June September 2013.
157. IICT, (2014), **Cyber-Terrorism Activities**, Report No. 8, ICT Cyber Desk, International Institute of Counter Terrorism, February 2013March 2014.
158. IMPC, (2014), Liking Facebook in Tehran: Social Networking in Iran, Iran Media Program Center for Global Communication Studies, Annenberg School for Communication, University of Pennsylvania, USA.
159. **Info, (2013),** Iran's Operation Saffron Rose Points to Increasing Cyber-Espionage Sophistication, Info-Security, Available at: http://www.infosecurity-magazine.com/news/irans-operation-saffron-rose-points-to-increasing/
160. INSS, (2014), **Executive Cyber Intelligence Bi-Weekly Report by INSS-CSFI**, Cyber Warfare Program, The Institute for National Security Studies, Tel Aviv, September 1st, 2014.
161. INSS, (2014), **Executive Cyber Intelligence**, Bi-Weekly Report by INSS-CSFI, December 15th, 2014.
162. INSS, (2014), **Executive Cyber Intelligence**, Bi-Weekly Report by INSS-CSFI, December 15th, 2014.
163. INSS, (2015), **Executive Cyber Intelligence**, Bi-Weekly Report by INSS-CSFI, April 1st, 2015.
164. ITIC,(2006),**Terrorism And Internet: An Examination Of Hamas's Websites And The Hosting Providers Used By Them**, Intelligence and Terrorism Information Center at the Center for Special Studies (C.S.S),Israel, (Updated to June 1, 2006).
165. ITO, (2014), **Measuring the Information Society of Iran (Islamic Rep.) 2014**, Information Technology Organization of Iran (ITO), Ministry of ICT, Tehran, IRAN.
166. ITO, (2015), **Measuring the Information Society of Iran (Islamic Rep.) 2015**, Ministry of ICT Information Technology Organization of Iran (ITO), Tehran, IRAN.
167. ITU, (2013), **ICT Measurement in Iran**, Document C/26-E, 11th World Telecommunication/ICT Indicators Symposium (WTIS-13) Mexico City, México, 4-6 December 2013.
168. ITU, (2014), **The State of Broadband 2014: Broadband for all: A report by the Broadband Commission**, International Telecommunication Union, September 2014.
169. ITU, (2015), **Cyber-wellness Profile: Iran**, International Telecommunication Union, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx.
170. ITU, (2015), **Global Cybersecurity Index & Cyber-wellness Profiles**, International Telecommunication Institute.

171. ITU,(2013), **ICT Measurement in Iran** , Ministry of Communications and Information Technology - IRAN, Document C/26-E , 11th World Telecommunication/ICT Indicators Symposium (WTIS-13) Mexico City, México, 4-6 December 2013.
172. IWS, (2015), **Iran Internet Usage, Broadband And Telecommunications Reports**, Middle East Internet Statistics, Internet World Statistics, http://www.internetworldstats.com/.
173. Jackson, K., (2012), **Iranian CERT Takes Center Stage with Flame**, Available at: http://www.darkreading.com/attacks-breaches/iranian-cert-takes-center-stage-with-flame/d/d-id/1137787.
174. Jackson, K., (2012), **Iranian CERT Takes Center Stage with Flame**, Available at: http://www.darkreading.com/attacks-breaches/iranian-cert-takes-center-stage-with-flame/d/d-id/1137787.
175. Jackson, K., (2012), **Iranian Hackers Claim They Compromised NASA SSL Digital Certificate**, Available At: http://www.darkreading.com/attacks-breaches/iranian-hackers-claim-they-compromised-nasa-ssl-digital-certificate/d/d-id/1137739.
176. Jackson, K., (2012,a), **Iranian Cyberthreat to U.S. A Growing Concern**, Available at: http://www.darkreading.com/vulnerabilities---threats/iranian-cyberthreat-to-us-a-growing-concern/d/d-id/1137586.
177. Jackson, K., (2014), **Anatomy of The New Iranian APT**, Available At: http://www.darkreading.com/anatomy-of-the-new-iranian-apt/d/d-id/1252695
178. Jackson, K., (2014), **Iranian Cyberspies Pose as Journalists Online to Ensnare Their Targets**, Available At: http://www.darkreading.com/attacks-breaches/iranian-cyberspies-pose-as-journalists-online-to-ensnare-their-targets/d/d-id/1269270
179. Jackson, K., (2014), **On The Trail of an Iranian Hacking Operation**, Available At: http://www.darkreading.com/analytics/threat-intelligence/on-the-trail-of-an-iranian-hacking-operation/d/d-id/1252723
180. Jahangard, N., (2004),TAKFA: **Iran's Road to Knowledge-based Development**, IRANDOC, Proceedings of the Meeting & workshop on Development of a National IT Strategy Focusing on Indigenous Content Development, Ministry of Science, Research & Technology Iranian Information & Documentation Center (Research Center), Iran-Tehran October, 2nd & 3rd Octobr,2004.
181. Janczewski, L., & A., Colarik, (2005), **Managerial Guide for Handling Cyber Terrorism & Information Warfare**, IDEA Group Publishing, London, UK.
182. Jawad, M.,(2014), **The Paradox of Higher Education in Iran**, Iran Pulse, The Middle East Pulse, Al-Monitor, Available At: http://www.al-monitor.com/pulse/home.html.
183. John, N. & S., Aytng, (2011), **The Business Year 2011: Iran**, London, U.K.
184. Jordan, T., (1999), **Cyber Power: The Culture and Politics of Cyberspace and The Internet**, Routledge, Francis & Taylor, London, UK.
185. Kadivar, M., (2014), **Cyber-Attack Attributes**, Technology Innovation Management Review, November 2014.
186. Kagan, F. & T., Stiansen, (2015), **The Growing Cyber Threat from Iran, The Initial Report Of Project Pistachio Harvest**, American Enterprise Institute Critical Threats Project and Norse Corporation, April 2015.
187. Kahn, K. & D. Kellner, (2009), **Oppositional Politics And The Internet: A Critical/ Reconstructive Approach**, Cultural Politics, Volume 1, Issue 1,Pp 75–100.

188. Kale, E., (2013), **Iranian Cyber War Commander Found Dead In The Woods**, TG Daily, October 5th 2013.
189. Katz, Y., (2011), **Iran Embarks on $1b. Cyber-Warfare Program**, Jerusalem Post, December 18, 2011.
190. Kelly ,J. & B. Etling,(2008), **Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere**, Internet & Democracy Case Study Series, Berkman Center Research Publication No. 2008-01, Berkman Center for Internet & Society, Harvard University.
191. Kelly, J. & B. Etling, (2009),**Mapping Change in the Iranian Blogosphere**, Internet & Democracy Blog, Berkman Center for Internet & Society, Harvard University.
192. Kelly, J., & B., Etling, (2008), **Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere**, No. 2008-01, Internet & Democracy Studies Series, Berkman Center Research Publication, The Berkman Center for Internet & Society, Harvard University.
193. Kelly, J., & B., Etling, (2008), **Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere**, Publication No. 2008-01, The Berkman Center for Internet & Society, Harvard University.
194. Khaksar, E., & A., Khaksar, (2015), **The Role of Open Source Software in Development of Software Industry in Developing Countries with Weak Intellectual Property Rights: the Case Study of Iran Local Operating System** , American journal of Systems and Software, 2015, Vol.3, No.1, 20-23.
195. Khanmesan, A., (2010), **e-Learning In Iran II**, Department of Education & Psychology, University of Birjand, Birjand, IRAN.
196. Khiabany, G., & A., Sreberny, (2007),**The Politics of/in Blogging in Iran**, Comparative Studies of South Asia, Africa and the Middle East, Vol. 27, No. 3, 2007.
197. Khiabany, G., & A., Sreberny, (2009), **The Internet in Iran: The Battle Over an Emerging Virtual Public Sphere**, Seminar, Yeungnam University, South Korea.
198. Knopová, M., & E., Knopová, (2014), **The Third World War? In The Cyberspace: Cyber Warfare in the Middle East**, Acta Informatica Pragensia, 3(1), 2014, pp.,23–32.
199. Kokhreidze, N., (2015), **Cyberspace and Cyber Warfare Capabilities of Iran**, Security AP., May 14, 2015.
200. Koomen, M., (2012), **Dissonance Online: The Islamic Republic of Iran, Music, and the Internet**, Master Thesis, Utrecht University.
201. Kredo, A., (2015), **Iran Steps Up Cyber Attacks Across the Globe**, The Washington Free Beacon, June 15th 2015.
202. Lake, E., (2012), **Did Iran's Cyber-Army Hack into the IAEA's Computers?**, The Daily Beast, Dec., 16th 2012.
203. Lake, E., (2012), **Did Iran's Cyber-Army Hack into the IAEA's Computers?**,The Daily Beast, Dec., 16th 2012.
204. Iasiello, E., (2015), **Are Cyber Weapons Effective Military Tools?,** Military & Strategic Affairs, Vol. 7, No. 1, March 2015.
205. Lasiello, E., (2015), **Preserving Power: Post-Sanction Financial Windfall Will Not Fuel Iran's Cyberwarfare Program**, EPOCH TIMES, Available at: http://www.theepochtimes.com.
206. LeClaire, L., (2015), **10 Ominous State Sponsored Hacker Groups**, Available At; http://listverse.com/2015/01/08/10-ominous-state-sponsored-hacker-groups/.
207. Lever, R., (2014), **Iran Cyber Spies Created Fake News Website, Researchers Say** (Update), PHYS.ORG, 29 May 2014.

208. Lewis, J., & K., Timlin, (2011), **Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization**, Center for Strategic and International Studies, Washington DC, USA.

209. Lewis, J., (2014), **Cybersecurity and Stability in the Gulf**, Middle East Program, Center for Strategic & International Studies, Washington, DC., USA.

210. Libicki, M., (2007), **Conquest in Cyberspace National Security and Information Warfare**, The RAND Corporation, Cambridge University Press, UK.

211. Libicki, M., (2009), **Cyberdeterrence and Cyberwar**, RAND Corp., USA.

212. Luce, D., (2015), **Iran Poses Growing Cyber Threat to US**, PHYS.ORG, 16 April 2015.

213. M.I.T.I.C, (2013), **Terrorism in Cyberspace: Hezbollah's Internet Network**, The Meir Amit Intelligence & Terrorism Information Center, The Israeli Intelligence & Heritage Commemoration Center, March 2013, Tel Aviv, Israel.

214. M.O.E, (2015), **Education for All 2015 National Review**: 2000-2015, Ministry of Education, Islamic Republic of Iran, Tehran.

215. M.o.ICT, (2015), **Measuring Information Society in Iran**, Information Technology Organization of Iran, Ministry of ICT, Tehran, Iran.

216. M.O.ICT,(2015), **The official Portal of Measuring Information Society in IRAN**, IRAN information Technology Organization , Ministry of ICT, Tehran, IRAN.

217. Macková , V., (2013), Cyber War Of The States: Stuxnet And Flame Virus Opens New Era Of War, Policy Paper, Cyber Security, CENNA, USA.

218. MAI, (2011), **Iran Calls on Islamic Hackers to Enlist to the Iranian "Cyber War"**, Available At: http://www.crethiplethi.com/.

219. Majlesi, A., (2015), **Iran to Implement Twin Smart Internet Filtering Projects**, Orient Press, http://www.orientswiss.com/.

220. Malcolm, P., (2015), **Iran Now Major Cyber-Threat**, Truth Revolt, David Horowitz Freedom Center, USA.

221. Mansharof , Y., (2013), **Iran's Cyber War: Hackers in Service of The Regime; IRGC Claims Iran Can Hack Enemy's Advanced Weapons Systems; Iranian Army Official: 'The Cyber Arena Is Actually The Arena Of The Hidden Imam'**, Series Report No. 1012, The Middle East Media Research Institute, Washington, DC., August 25,2013.

222. Martin, J., (2012), **Information Center's Cyber Intelligence Report (CIR)**, Information Warfare Center, USA.

223. Martin, J., (2012), **Information Center's Cyber Intelligence Report (CIR)**, Information Warfare Center, USA.

224. Masoumi, D., (2010), **Quality in E-learning Within a Cultural Context: The Case of Iran**, Thesis, University of Gothenburg, Sweden.

225. May 10, 2013.

226. McInnis, J., (2015**), Iran's Strategic Thinking: Origins and Evolution**, American Enterprise Institute, USA.

227. Mehrara, M., Amiri, R., & Z., Falahati, (2013), **Performance of Iran's Sustainability Index as Compared to the Global Average,** American Research Institute for Policy Development, Journal of Economics and Development Studies, Vol. 1 No. 3, December 2013.

228. Mele, S., (2013), **Cyber-Weapons: Legal and Strategic Aspects**, Italian Institute of Strategic Studies, Milano, Italy.

229. Middleton, B., (2004), **Cyber Crime Investigator's Field Guide**, Second Edition, Auerbach Publications, New York, USA.
230. Mina, N., (2010), **Blogs, Cyber-Literature and Virtual Culture in Iran**, No. 15, Occasional Papers, George C. Marshall Center, Germany.
231. MohammadJavadi, M., & S., Saadi, (2010), **Medical Informatics in IRAN**, Available at: http://journals.sbmu.ac.ir/jps/article/viewFile/2224/1906.
232. Mohebali, A., & M., Rezam, (2014), **Measuring ICT Access and Use by Households and Individuals in Iran**, Iran ICT Ministry of Information Technology Organization (ITO), 2ndMeeting of the Expert Group on ICT Household Indicators (EGH), ITU, Geneva, 15-16 September 2014.
233. MoICT, (2015), **E-Government development roadmap of I.R. of Iran, The Bylaw of Development of e-Services of Executive Bodies**, Ministry of ICT, Iran.
234. MoICT, (2015), **Measuring the Information Society of Iran 2015: ICT and Sustainable Development**, Ministry of ICT, Tehran, Iran.
235. MOSAIC, (1999), **The Global Diffusion of Internet – 1998, Iran**, URL: mosaic.unomaha.edu/GDI1998/IRAN.
236. MPO, (2005), **Law of the Fourth Economic, Social & Cultural Development Plan of the Islamic Republic of Iran – Tehran**, Management Planning Organization, Deputy for Administrative, Financial & Human Resources Affairs, Center for Documentation, Museum & Publications, Tehran, Iran.
237. Naeli, M., (2013), **New Trends of Social Media Use in Iran: Candidates' Campaigns on Social Networks in the 2013 Presidential Election**, Global Media Journal, Vol. 3, No. 2, Autumn/Winter 2013.
238. Nafisi ,A.,(2008), Blogging Outside Iran: A Tool for Internal Democratic Change? ,Communication 497 Honors Thesis, June 13, 2008.
239. Najafi, S., Ahmadzadeh-Raji, M., Fathollahi, J. , Dadkhah, V. & Z., Faryadi, (2013), **Iran and Knowledge Creation Infrastructures in the Knowledge Economy Era**, Journal of Basic and Applied Scientific Research, 3(6)783-796, 2013.
240. Nakashima, E., (2014), **Iranian Hackers are Targeting U.S. Officials Through Social Networks**, Report Says, National Security, USA.
241. Nakashima, E., Miller, G., & J., Tate, (2012), **U.S., Israel developed Flame Computer Virus to Slow Iranian Nuclear Efforts**, The Washington Post, June,19, 2012.
242. NATO, (2013), **Cyber Attacks Timeline**, NATO Review Magazine, Available at: http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm.
243. Nazarian, A., (2015), **California Man Discovers Iranian Hackers in Power Grid**, BRIETBART, Dec., 21st 2015.
244. Nazarian, A., (2015), **California Man Discovers Iranian Hackers in Power Grid**
245. NCTB,(2007), **Jihadis and The Internet**, The National Coordinator of Counterterrorism, USA.
246. NED,(2009), **A Guide to New Media in Iran**, Center for International Media Assistance, USA.
247. Nguyen, R., (2013), **Navigating Jus Ad Bellum in the Age of Cyber Warfare**, Article 4, Volume 101, Issue 4, California Law Review.
248. Niayesh, U., (2015), **Iran to launch second phase of smart filtering in two months**, Azer News, 4 May 2015, http://en.trend.az/.
249. Nicholson, B., & S., Sahay, (2003), **Building Iran's Software Industry: An Assessment of Plans and Prospects Using the Software Export Success Model,**

Working Paper Series, Paper No.15, Institute for Development Policy and Management, University of Manchester, Precinct Centre, Manchester, UK.

250. Nightingale, R., (2015), **4 Top Hacker Groups and What They Want**, Available At: http://www.makeuseof.com/tag/4-top-hacker-groups-want/.

251. NS,(2011), **Iran is Top of The World in Science Growth**, New Scientist, March, 2011.

252. NUFFIC, (2015), **Education System in Iran**, EP-NUFFIC, 2nd Edition, NUFFIC Organization, Netherlands.

253. Nye, J., (2010), **Cyber Power**, Harvard Kennedy School, BELFER Center for Science & International Affairs, USA.

254. OB, (2013), **Iran's Cyber Posture**, Intelligence Brief, Open Briefing, 8 November 2013.

255. O'Connell, J., (2015), **10 Most Notorious Hacking Groups of All Time**, Hacked, Available At: https://hacked.com/.

256. Omidinia, S., Masrom, M., & H., Selamat, (2010),**A Review on E-learning Development and Implementation in Developing Countries (Case Study of Iran),** Faculty of Computer Science and Information System, University Technology, Malaysia (UTM).

257. ONI, (2005), **Internet Filtering in Iran in 2004-2005: A Country Study**, Open Net Initiative, Harvard University.

258. ONI, (2009), **Internet Filtering in Iran**, Open Net Initiative, Harvard University, USA.

259. ONI, (2013), **After the Green Movement: Internet Controls In Iran, 2009-2012**, Open.net Initiative, February, 2013.

260. Open Net,(2009), **Internet Filtering in Iran**, Open Net Initiative, Refer to URL : http://opennet.net/studies/iran2009.

261. ORN, (1999), **Iran's Telecom and Internet Sector: A Comprehensive Survey**, Open Research Network, Tarzana, USA.

262. Osipova, Y., (2011), **Hizballah's Media Strategy: Creating a "Theater of Terror"**, Journal of International Service, Fall 2011.

263. Otafu, B., Bamodu, O., Tian, L. & U., Otafu, (2013), **Use of Internet and Associated Technologies in "Cyber-Warfare" and Issues Affecting its Investigation**, International Conference on Education Technology and Information System (ICETIS 2013).

264. Otafu, B., Bamodu, O., Tian, L. & U., Otafu, (2013), **Use of Internet and Associated Technologies in "Cyber-Warfare" and Issues Affecting its Investigation**, International Conference on Education Technology and Information System (ICETIS 2013).

265. Parsa, W., (2008), **Weblogistan: A New Path to Self-Expression in Iran**, Occasional Paper, Konrad - A denauer – Stiftung, Washington, D.C., USA.

266. Parteni, L.,(2009), **Twitter Delays Downtime to Enable Iranian Protests to Continue**, SOFTPEDIA, June 16th 2009.

267. Patterson, J., & M., Smith , (2005), **Developing A Reliable Methodology for Assessing The Computer Network Operations Threat of Iran**, Naval Postgraduate School, September 2005, USA.

268. Pavel,T.,(2009), **The Power of 140 Characters: Twitter in the Middle East**, Tel Aviv Notes, July 26, 2009.

269. Payvand, (2010), **Internet Speed Test Ranks Islamic Republic of Iran 168 out of 181 Countries,** http://payvand.com/blog/blog/2010/08/08/internet-speed-test-ranks-islamic-republic-of-iran-168-out-of-181-countries/

270. Perlroth, N., (2014), **Report Says Cyberattacks Originated Inside Iran**, The Washington Post, Dec. 2, 2014.
271. Pessin, A., (2015), **Cyber War Rages Between Iran, US**, VOA, March, 23rd 2015.
272. Porter, G., (2010), **Iran Places Trust in 'Passive Defense', Middle East,** Asia Times, Jan. 13th 2010.
273. Price, M., (2012), **Iran and the Soft War**, International Journal of Communication 6 (2012), Feature 2397–2415.
274. Prince, B., (2014), **Iranian-Sponsored Hackers Hit Critical Infrastructure Companies: Research**, Security Week, Dec. 2nd 2014.
275. PTV, (2010), **Iran's Science Progress Fastest In World: Canadian Report,** Available at http://edition.presstv.ir/detail/118977.html.
276. Raboin, B., (2011), **Corresponding Evolution: International Law and the Emergence of Cyber Warfare**, Journal of The National Association of Administrative Law Judiciary, Article 5, Vol. 31, Issue 2.
277. Rafizadeh, S., & M., Alimardani, (2013), **Facebook, Twitter, and Protests: 2009 and 2013**, The Iran Media Program, URL: http://iranmediaresearch.org/.
278. Rahimi,B.,(2003), Cyberdissent: **The Internet In Revolutionary Iran**, Middle East Review of International Affairs Journal, Volume 7, No. 3 - September 2003.
279. Rahmani, G., (2013), **Iran to Improve the Facilities of its Datacenters**, Pars Herald, http://parsherald.com/iran-to-improve-the-facilities-of-its-datacenters/1339/.
280. Rasoulian , M., & M., Safari, (2011), **The Reasons To Lack Of Electronic Banking Achievement In Iran,** International Journal of Managing Information Technology (IJMIT) Vol.3, No.3, August 2011.
281. Ray, C., (1997), **Cyberwar and Information Warfare: A Revolution in Military Affair! Or Much Ado About Not Too Much**?, National War College, National Defense University, USA.
282. ReneSys, (2015), **Iran: Latest Nation to Host Critical Global Internet Infrastructure**, Internet Intelligence, Dyn Research, USA.
283. Reuters, (2015**), Iranian Hackers Targeted Israeli Nuclear Scientists, Security Researchers Say**, Technology, Available at: http://www.ynetnews.com/home/0,7340,L-3083,00.html.
284. Reyes, A., (2007), **Cyber Crime Investigations: Bridging the Gaps, Between Security Professionals, Law Enforcement, and Prosecutors**, Syngress Publishing, Inc., Rockland, MA, USA.
285. Rezaian, J., (2014), **Internet Improvements in Store for Iran**, The Middle East, The Washington Post, February 15, 2014.
286. Rezvaniyeh, F., (2010), **Report on the Operation of the Iran Cyber Army in Hacking Websites**, Avaialble at: www.kaleme.com
287. Rezvaniyeh, F., (2010), **Report on the Operation of the Iran Cyber Army in Hacking Websites**, Avaialble at: www.kaleme.com
288. Rhoads, C., & F., Fassihi, (2011), **Iran Vows to Unplug Internet**, TECH, , The Wall Street journal, May 28, 2011.
289. Richardson , J., (2011), **Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield**, JMR Portfolio Intelligence, Inc., Washington, DC., USA.
290. Rigby, A., (2007), **Looking for Freedom: An Exploration of the Iranian Blogosphere,** Thesis, The University Of Sheffield, UK.
291. Robertson, B., & J., Marchant, (Editors), (2014), **Revolution Decoded: Iran's Digital Landscape**, Small Media Organization.

292. Rodriguez, E., Hoskins, A., & M., Tapia, (2015), **DISEC Cyberwarfare**, Carmelitas College, UN.

293. Rokni, M., (2005), **E-learning in Type 1 Medical Universities of Iran**, Turkish Online Journal of Distance Education-TOJDE July 2005 ISSN 1302-6488 Volume: 6, Number: 3 Article No: 2.

294. Rosenzweig, P., (2013),**Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World**, PRAEGER, Santa Antonio, USA.

295. Rowen, B., (2015), **Cyberwar Timeline: The Roots Of This Increasingly Menacing Challenge Facing Nations And Businesses**, Infoplease, Available At:

296. Runkle, B., (2015), **Opinion: Why Iran Is Sharpening Its Cyber-Arms Arsenal**, The Christian Science Monitor, Dec., 9, 2015.

297. S.C.I,(2012), **Selected Findings of the 2011 National Population & Housing Census**, Statistical Center of IRAN, Tehran, IRAN.

298. Salvin, B., & J., Healy, (2014), **Iran: How a Third Tier Cyber Power Can Still Threaten the United States,** Brent Scowcroft Center On International Security, South Africa Center.

299. Sam, B., & L., DeNardis, (2012), **The Politicization of the Internet's Domain Name System**: **Implications for Internet Security**, Universality, and Freedom, Unpublished Manuscript, USA.

300. Samiee, M., & K., Davallu, (2014), **The Strategic Programme for the Management of Digital Preservation of Governmental Records,** IFLA, Lyon, 2014.

301. Sanati, K., (2009), **MEDIA-IRAN: Policing of Internet Will Continue**, IPS, Inter Press Service News Agency, The Story Underneath, Friday, May 29, 2.

302. Sandoval, L., (2014), **Iranian Hacking Group Ajax Security Team Shows Aggressiveness, Targets U.S. Defense Firms: Fire-eye**, Tech Times, Available at: http://www.techtimes.com/

303. Sanger, D., (2015), **Document Reveals Growth of Cyberwarfare Between the U.S. and Iran**, New York Times, Feb., 22nd 2015.

304. Sanger, D., (2016), **U.S. Indicts 7 Iranians in Cyberattacks on Banks and a Dam The New York Times**, The New York Times, March, 24th , 2016.

305. Sawahel, W.,(2009), **Iran: 20-Year Plan for Knowledge-based Economy**, University world News, 30th August,2009, Available on: http://www.universityworldnews.com/.

306. Scharr, J., (2014), **Iran Blamed for 'Saffron Rose' Cyberespionage Campaign**, TOMSGUIDE, Available at: http://www.tomsguide.com/us/iran-cyberespionage-saffron-rose,news-18779.html.

307. Schwartz, M., (2011), **Iran Alleges Espionage Over Internet Worm**, Available At:

308. Schwartz, M., (2012), **U.S. Bank Attackers Dispute Iran Ties**, Available At: http://www.darkreading.com/attacks-and-breaches/us-bank-attackers-dispute-iran-ties/d/d-id/1107584.

309. Schwartz, M., (2012,a), **Malware Corrupts Iranian Financial Databases**, Available At: http://www.darkreading.com/risk-management/malware-corrupts-iranian-financial-databases/d/d-id/1107525

310. Schwarz, D., (2013), **INSS Article: Iran on The Cyber Offensive**, Israel's Homeland Security Home, Tel Aviv, Israel.

311. Schwarz, D., (2013), **INSS Article: Iran on The Cyber Offensive**, iHLS, Israel's Homeland Security, Jan. 7, 2013.

312. Schwarz, D., (2013), **INSS Article: Iran on The Cyber Offensive**, iHLS, Israel's Homeland Security, Jan. 7, 2013.
313. Schwarz, D., (2013), **INSS Article: Iran on The Cyber Offensive**, Israel's Homeland Security Home, Tel Aviv, Israel.
314. Schwarz, D., (2013), **INSS Article: Iran on The Cyber Offensive**, iHLS, Israel's Homeland Security, Jan. 7, 2013.
315. Schwarz, D., (2013), **INSS Article: Iran on The Cyber Offensive**, iHLS, Israel's Homeland Security, Jan. 7, 2013.
316. Schwarz, D., (2013), **INSS Article: Iran on The Cyber Offensive**, Israel's Homeland Security Home, Tel Aviv, Israel.
317. Schwarz, D., (2013), **INSS Article: Iran on The Cyber Offensive**, iHLS, Israel's Homeland Security, Jan. 7, 2013.
318. Semati, M., (2008),(Editor), **Media, Culture And Society In Iran:** Living With Globalization And The Islamic State, Routledge, Oxon, Canada.
319. Semati, M., (Editor),(2008), **Media, Culture and Society in Iran: Living with Globalization and the Islamic State**, Routledge, Oxon, Canada.
320. Sennhauser, M., (2009), **The State of Iranian Communication: Manipulation and Circumvention**, Public Release, Version 1.2.1, Nedat Project.
321. Sennhauser, M.,(2009), **The State Of Iranian Communication: Manipulation And Circumvention**, NedaNet, July 13th 2009.
322. Sennhauser, M.,(2009), **The State Of Iranian Communication: Manipulation And Circumvention**, NedaNet, July 13th 2009.
323. SenseCy, (2014), **Iranian Hackurity – Hacking Group or Security Firm**, Available at: https://blog.sensecy.com/.
324. Shackelford, S., (2013), **Toward Cyber-peace: Managing Cyberattacks through Polycentric Governance**, American University Law Review 62, no.5 (2013): 1273-1364.
325. Shadanpour, F., Dariyan, S., Farahani, R., Seirafi, & S., Vazifehdoust (2012), **Building an Iran Web Archive in the National Library and Archives of Iran: A Feasibility Study**, Library Philosophy and Practice 2012.
326. Shaheed, A., (2015), **Iran: Defending from the Outside Needs Assessment of Iranian Human Rights Defenders in the Diaspora**, Article No. 19, Country Report, Free World Centre, London, UK.
327. Shahghasemi, E., Tafazzoli, B., Akhavan, M., Mirani, G., & T., Khairkhah, (2013),
328. Shakarian, P., (2011), **Stuxnet: Cyberwar Revolution in Military Affairs,** Small Wars Foundation, April 15, 2011.
329. Shakarian, P., Shakarian, J., & A., Ruef, (2013), **To Cyber-Warfare: A Multidisciplinary Approach**, Elsevier, Inc., Amsterdam, Holland.
330. Shakarian, P., Shakarian, J., & A., Ruef, (2013), **To Cyber-Warfare: A Multidisciplinary Approach**, Elsevier, Inc., Amsterdam, Holland.
331. Shakarian, P., Shakarian, J., & A., Ruef, (2013), **To Cyber-Warfare: A Multidisciplinary Approach**, Elsevier, Inc., Amsterdam, Holland.
332. Shakarian, P., Shakarian, J., & A., Ruef, (2013), **To Cyber-Warfare: A Multidisciplinary Approach**, Elsevier, Inc., Amsterdam, Holland.
333. Shakarian, P., Shakarian, J., &A., Ruef, (2013), **To Cyber-Warfare: A Multidisciplinary Approach**, Elsevier, Inc., Amsterdam, Holland.
334. Sheldon, J., (2011), **Deciphering Cyber-power: Strategic Purpose in Peace and War**, Strategic Studies Quarterly, Summer 2011.

335. Siboni, G. & S., Kronenfeld , (2014), **Iran and Cyber Warfare**, In (Editor: Gabi Siboni): Cyberspace and National Security Selected Articles, Center for Strategic Studies, INSS Project, Israel.
336. Siboni, G., & and S.,Kronenfeld, (2014), **Developments in Iranian Cyber Warfare 2013-2014**, Military and Strategic Affairs, Volume 6 ,No. 2 ,August 2014.
337. Siboni, G., & S., Kronenfeld, (2012), **Iran's Cyber Warfare**, INSS Insight No. 375, October 15, 2012.
338. Siboni, G., & Z., Magen, (2016), **The Cyber Attack on the Ukrainian Electrical Infrastructure: Another Warning**, INSS Insight No. 798, February 17, 2016.
339. Siboni, G., (2011), **Protecting Critical Assets and Infrastructures from Cyber Attacks,** Military and Strategic Affairs , Vol. 3, No.1 , May 2011.
340. Siboni, G., et.,al.,, (2015), **Operation Cleaver**, Cylance Inc., USA.
341. Siboni, G.,& S., Kronenfeld, (2014), **Developments in Iranian Cyber Warfare 2013-2014**, Military & Strategic Affairs, Vol.6, No.2, August 2014.
342. Siboni, G.,&S., Kronenfeld, (2012), **Iran and Cyberspace Warfare**, Military and Strategic Affairs, Volume 4, No. 3, December 2012, pp.77-99.
343. Siboni, G.,&S., Kronenfeld, (2014), **Developments in Iranian Cyber Warfare 2013-2014**, Military & Strategic Affairs, Vol.6, No.2, August 2014.
344. Siboni, K., & S., Kronenfeld, (2014,), **The Iranian Cyber Offensive during Operation Protective Edge, INSS Insight** No. 598, August 26, 2014.
345. Sigholm, J., (2013), **Non-State Actors In Cyberspace Operations**, Swedish National Defense College, Sweden.
346. Simpson, E., (2015), **North Korea's Attack on Sony Pictures Gets the Headlines, But Many Countries Are Engaged in This New War Front**, Paper 78, Political Science Publication, Western University, Canada.
347. Slavin, B., & J., Healy, (2013), **Iran: How a Third Tier Cyber Power Can Still Threaten the United States**, Issue Brief, Atlantic Ocean, USA.
348. SM, (2014), **Iranian Internet Infrastructure and Policy Report**, September 2014, smallmedia.org.uk.
349. Small-Media, (2014), **Websites and Service Competition: Iran Vs. The West,** Iranian Internet Infrastructure and Policy Report, July 2014, Smallmedia.Org.Uk.
350. Small-Media, (2014), **Websites and Service Competition: Iran Vs. The West,** Iranian Internet Infrastructure and Policy Report, July 2014, Smallmedia.Org.Uk.
351. Small-Media, (2014), **Websites and Service Competition: Iran Vs. The West,** Iranian Internet Infrastructure and Policy Report, July 2014, Smallmedia.Org.Uk.
352. SMO, (2013,a), **Iranian Internet Infrastructure and Policy Report**, August-September 2013 Issue, Small Media Organization, Smallmedia.org.uk.
353. SMO, (2013,b), **Iranian Internet Infrastructure and Policy Report**, December 2013 Issue, Small Media Organization, Smallmedia.org.uk.
354. SMO, (2014,a), **Iranian Internet Infrastructure and Policy Report** , January 2014 Issue, Small Media Organization, Smallmedia.org.uk.
355. SMO, (2014,b), **Iranian Internet Infrastructure and Policy Report** , April 2014 Issue, Small Media Organization, Smallmedia.org.uk.
356. SMO, (2014,b), **Iranian Internet Infrastructure and Policy Report** , April 2014 Issue, Small Media Organization, Smallmedia.org.uk.
357. SMO, (2014,c), **Iranian Internet Infrastructure and Policy Report** , July 2014 Issue, Small Media Organization, Smallmedia.org.uk.

358. SMO, (2014,c), **Iranian Internet Infrastructure and Policy Report** , July 2014 Issue, Small Media Organization, Smallmedia.org.uk.

359. SMO, (2015,a), **Iranian Internet Infrastructure and Policy Report** , February 2015 Issue, Small Media Organization, Smallmedia.org.uk.

360. SMO, (2015,b), **Iranian Internet Infrastructure and Policy Report** , June 2015 Issue, Small Media Organization, Smallmedia.org.uk.

361. SMO, (2015,c), **Iranian Internet Infrastructure and Policy Report** , July 2015 Issue, Small Media Organization, Smallmedia.org.uk.

362. Snapshots, (2015), **Iran Increases Cyberattacks Against the United States; Where's the Coverage?**, SNAPSOHTS A CAMERA BLOG, Available At: http://blog.camera.org/.

363. Soofi, A., & S., Ghazinoory, Editors,(2013), **Science & Innovations in Iran: Development, Progress & Challenges**, Palgrave McMillan, New York, USA.

364. Srebenry, A., & G., Khiabany, (2008), **Being Intellectual: The Blogestan & Public Political Space in the Islamic Republic**, In: **Iranian Intellectuals 1997-2007**, Routledge, Oxon, USA.

365. Stodden, V., (2009), **Openness and The Internet Explosion in Iran**, Berkman Center for Internet & Society, Harvard University.

366. Symantec, (2015), **Iran-Based Attackers Use Back Door Threats to Spy on Middle Eastern Targets**, Symantec Official Blog, Symantec Inc., USA.

367. Tabesh, Y., Khansuri, M., Zarkalam, S., Saljooghi, K., Pour, H., & P., Naaseri, (2004), **IRANDOC-Digital Review of Iran**, Proceedings of The Meeting & Workshop on the Development of a National IT Strategy Focusing on Indigenous Content Development, Tehran, Iran.

368. TDS, (2014), **Iranian President Urges Religious Leaders to Tolerate Internet**, Middle East, The Daily Star, September 1st 2014, Lebanon.

369. **Technology Report 2014: Rewards and Risks of Big Data**, World Economic Forum, Geneva.

370. **Technology Report 2014: Rewards and Risks of Big Data**, World Economic Forum, Geneva.

371. **Technology Report 2015: ICTs for Inclusive Growth**, Insight Report, World Economic Forum, Geneva.

372. **Technology Report 2015: ICTs for Inclusive Growth**, Insight Report, World Economic Forum, Geneva.

373. Thornburgh, N., (2005), **The Invasion Of The Chinese Cyber Spies: An Exclusive Look at How The Hackers Called TITAN RAIN Are Stealing U.S. Secrets**, 29 August, Time Magazine [online], Available: http://courses.cs.washington.edu/courses/csep590/05au/ readings/titan.rain.htm.

374. TIS, (2016), **Israeli Generals Said Among 1,600 Global Targets of Iran Cyber-Attack**, Times of Israel, January, 28th 2016.

375. TN, (2015), **100 Hackers Arrested in Iran in one Month** , Tehran News, Nov. 16,2015.

376. Tower, (2015), **Israeli Cyber Expert: Hackers, Not Suicide Bombers, Will Cause Next 9/11, IRAN**, Tower Organization, http://www.thetower.org/1892-israeli-cyber-expert-hackers-not-suicide-bombers-willcause-next-911/.

377. Tower, (2015), **Israeli Cyber Expert: Hackers, Not Suicide Bombers, Will Cause Next 9/11**, IRAN, Tower Organization, http://www.thetower.org/1892-israeli-cyber-expert-hackers-not-suicide-bombers-willcause-next-911/.

378. TSOS, (2014), **Operation Saffron Rose: Iranian Hacker Group Targeting U.S. Defense Orgs & Dissidents**, The State of Security, Available at: http://www.tripwire.com/state-of-security/latest-security-news/operation-saffron-rose-iranian-hacker-group-targeting-u-s-defense-orgs-dissidents/.
379. UN, (2003), **Declaration of Principles: Building the Information Society: a Global Challenge in the New Millennium,** Plan of Action, WSIS-03/GENEVA/DOC, World Summit on the Information Society, December 12th 2003, United Nations, Geneva.
380. UN, (2013), **The Cyber Index International Security Trends and Realities**, United Nations, USA.
381. UN, (2014), **E- Government for the Future We Want, United Nations E-Government Survey 2014**, United Nations Department of Economic and Social Affairs, UN, New York, USA.
382. UNDP, (2014), **Human Development Report 2014- Sustaining Human Progress: Reducing Vulnerabilities and Building Resilience**, United Nations Development Programme, New York, USA.
383. UNESCO, (2005), **Towards Knowledge Societies**, UNESCO World Report, United Nations Educational, Scientific and Cultural Organization, Paris.
384. UNICEF, (2000), **Defining Quality in Education,** Working Paper Series , Education Section, Programme Division , The International Working Group on Education, Florence, Italy, June 2000.
385. UNICEF, (2000), **Defining Quality in Education,** Working Paper Series , Education Section, Programme Division , The International Working Group on Education, Florence, Italy, June 2000.
386. UNIDIR, (2013),**The Cyber Index: International Security Trends and Realities**, UNIDIR/2013/3, United Nations Institute for Disarmament Research, Geneva, Switzerland.
387. Valdini, C., (2012), **Saudi Hackers Target Iran Oil Sector – Report**, Available at: http://www.arabianbusiness.com/.
388. Valibeigi, N., (2012), **Manifestation of Religious Authority on the Internet: Presentation of Twelver Shiite Authority in the Persian Blogosphere**, Master Thesis, Waterloo, Ontario, Canada.
389. Vargas, D., & E., Vincze, (2015), **Hacktivism and The Rise of The Patriotic Hacker**, High Technology Crime Investigation Program, The George Washington University, USA.
390. Ventre, D., (Editor), (2011), **Cyberwar and Information Warfare**, John Wiley & Sons, New York, USA.
391. Ventre, D., (Editor), (2011), **Cyberwar and Information Warfare**, John Wiley & Sons, New York, USA.
392. Vijayan, J., (2015), **Experts Separate Fact from Hype in Reports of Iranian Hacking**, The Christian Science Monitor, Dec. 24th 2015.
393. Villeneuve, N., Moran, N., Haq, T., & M., Scott, (2013), **Operation Saffron Rose**, Special Report, Security Reimagined, FIREYE.
394. Villeneuve, N., Moran, N., Haq, T., & M., Scott, (2013), **Operation Saffron Rose**, Special Report, Security Reimagined, FIREYE.
395. Villeneuve, N., Moran, N., Haq, T., & M., Scott, (2013), **Operation Saffron Rose**, Special Report, Fire Eye, USA.
396. Walls, M., (2015), **Why Iran Hacks**, PERIMETER, Information Week, Dark reading, Jan,29th 2015.

397. Walls, M., (2015,a), **Nation-State Cyberthreats: Why They Hack**, Security Monitoring, Information Week, Dark Reading, August 1st 2015.
398. Waqas, (2016), **Official Web Portal of Supreme Leader of Iran Ruhollah Khomeini Hacked**, Available At; https://www.hackread.com/web-portal-of-iran-supreme-leader-khomeini-hacked/.
399. WB, (2015), **Iran: An Overview**, The World Bank, Available at: http://www.worldbank.org/, Last Updated on March, 2015.
400. WB, (2015), **Iran: An Overview**, The World Bank, Available at: http://www.worldbank.org/, Last Updated on March, 2015.
401. Webster, F., (2006), **Theories of the Information Society,** Third edition, Routledge, London, UK.
402. Webster, F., (2006), **Theories of the Information Society,** Third edition, Routledge, London, UK.
403. Wei, W., (2016), **The 7 Most Wanted Iranian Hackers By The FBI**, The Hacker News, Available At: http://thehackernews.com/2016/03/fbi-wanted-hackers.html
404. WEP,2009, **The Iranian Election on Twitter: The First Eighteen Days**, Pub.1, WEB Ecology Program, USA.
405. WEP,2009, **The Iranian Election on Twitter: The First Eighteen Days**, Pub.1, WEB Ecology Program, USA.
406. Wheeler, A., (2013), **The Iranian Cyber Threat**, Available At: http://phoenixts.com/blog/the-iranian-cyber-threat-part-1-irans-total-cyber-structure/.
407. Wheeler, A., (2013), **The Iranian Cyber Threat**, Available At: http://phoenixts.com/blog/the-iranian-cyber-threat-part-1-irans-total-cyber-structure/.
408. Wheeler, A., (2013), **The Iranian Cyber Threat**, Available At: http://phoenixts.com/blog/the-iranian-cyber-threat-part-1-irans-total-cyber-structure/.
409. Wheeler, A., (2013), The Iranian Cyber Threat, Phoenix, Available at: http://phoenixts.com/.
410. Wheeler, A., (2013), **The Iranian Cyber Threat**, Phoenix, Available at: http://phoenixts.com/.
411. Wheeler, A., (2013), **The Iranian Cyber Threat**, Phoenix, Available at: http://phoenixts.com/.
412. Wheeler, A., (2013), **The Iranian Cyber Threat**, Phoenix, Available at: http://phoenixts.com/.
413. WHO, (2012), **E-Health in Iran**, WHO Eastern Mediterranean Region.
414. Wikipedia, (2015), **Communications in Iran**, Wikipedia, Last Updated on May 2015.
415. Wikipedia, (2015), **Higher Education in Iran**, Wikipedia, Last Updated on July,2015.
416. Wikipedia, (2015), **Higher Education in Iran**, Wikipedia, Last Updated on July,2015.
417. Wikipedia, (2015), **Iran National Science Foundation,** Wikipedia, Last Updated on July,2015.
418. Wikipedia, (2015), **Iran National Science Foundation,** Wikipedia, Last Updated on July,2015.
419. Wikipedia, (2015), **Iran's National Elite Foundation**, Wikipedia, Last Updated on July,2015.
420. Wikipedia, (2015), **Iran's National Elite Foundation**, Wikipedia, Last Updated on July,2015.

421. Wikipedia, (2015), **Languages used on The Internet**, Wikipedia.
422. Wikipedia, (2015), **Science & Technology in Iran**, Wikipedia, Last Updated on July 2015.
423. Wikipedia, (2015), **Science & Technology in Iran**, Wikipedia, Last Updated on July 2015.
424. Wilhelmsen, V., (2014), **Soft War in Cyberspace: How Syrian Non-State Actors Use Hacking To Influence The Conflict's Battle Of Narratives**, Master's Thesis Political Science, Department Of Political Science, University Of Oslo.
425. Williams, J., (2014), **The New Target for State-Sponsored Cyber Attacks: Applications**, ATTACKS/BREACHES, Information Week, Dark Reading, Dec., 17th 2014.
426. Wilson, T., (2010), **Iran Arrests 30 Accused of U.S.-Backed 'Cyberwar'**, Available At: http://www.darkreading.com/government/cybersecurity/iran-arrests-30-accused-of-us-backed-cyberwar/d/d-id/1133213.
427. Wilson, T., (2012), **U.S. Defense Secretary Sends Veiled Warning to Iran**, Available At: http://www.darkreading.com/government/cybersecurity/us-defense-secretary-sends-veiled-warning-to-iran/d/d-id/1138518.
428. Worthen ,B., Esterl ,M. & S. Gorman, (2009), **Iran's Web Spying Aided By Western Technology**, Technology, June,22Th ,2009.
429. Worthen ,B., Esterl ,M. & S. Gorman, (2009), **Iran's Web Spying Aided By Western Technology**, Technology, June,22Th ,2009.
430. Yaghoubi, J., Mohammadi, M., Iravani, H., & A., Gheidi, (2008),**Virtual Students' Perceptions Of E-Learning In Iran**, The Turkish Online Journal Of Educational Technology – Tojet July 2008, Volume 7, Issue 3, Article 10.
431. Zamaneh, R., (2014), **Iran's National Internet to be Tested in Qom before Countrywide Roll-out**, Payvand Iran News, December 25th 2014.
432. Zeleti , F., (2010), **The Progress and Obstacles of Implementing and Improving E-Government in Islamic Republic of Iran**, Master's Thesis, Department of Information Technology, Faculty of Technology Management, Lappeenranta University of Technology, Sweden.
433. Zimmt, R., (2010), **Spot on Iran**, Intelligence & Terrorism information Center, IDF, Tel Aviv, Israel.
434. Zimmt, R., (2010), **Spot on Iran**, Intelligence & Terrorism information Center, IDF, Tel Aviv, Israel.
435. Zimmt, R., (2010), **Spot on Iran**, Intelligence & Terrorism information Center, IDF, Tel Aviv, Israel.
436. Zuckerman, E., Roberts, H., McGrady, R., York, J., & J., Palfrey, (2010), **Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites**, The Berkman Center for Internet & Society at Harvard University, USA.
437. Zurich, (2012), **HACKTIVISM: The Growth and Implications of this 21st Century Method of Protest**, White Paper, Advisen, Insurance Intelligence, Zurich.